

# Cybersecurity

## Awareness Campaign **Toolkit**



Organization of  
American States | More rights  
for more people

The Organization of American States (OAS) is the main political forum of the Region that promotes and supports Democracy, Human Rights, Multidimensional Security and Integral Development in the Americas. The OAS seeks to prevent conflicts and to bring political stability, social inclusion and prosperity to the region through dialogue and collective action such as cooperation, the implementation of follow-up mechanisms of the Member States engagements and the enforcement of Inter-American Law and International Law.

*This toolkit was created thanks to the financial support of the Governments of Canada and the United Kingdom.*

#### All rights reserved

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/igo/legalcode>.



#### Disclaimer

*The contents of this publication do not necessarily reflect the views or policies of the OAS or contributory organizations.*

**October 2015**

© OAS Secretariat for Multidimensional Security  
1889 F Street, N.W., Washington, D.C., 20006  
United States of America  
[www.oas.org/cyber/](http://www.oas.org/cyber/)

# Cybersecurity

## Awareness Campaign **Toolkit**



Organization of  
American States | More rights  
for more people

# Table of contents

Introduction		6
• Background		7
• Instructions		9
The Awareness & Education Continuum		10
The Campaign Structure	K	12
The Message	L	14
The Campaign Planner		18
• Stakeholders	H	20
• Goals		22
• Audience	D E F G	24
• Situation Analysis	K	26
• Strategy	A B	28
• Tactics	C I J	30
• Success		34
Putting it Together	A B D E F G	38

## Appendix

<b>A</b>	Campaign Strategies	<b>40</b>
<b>B</b>	Media Relations Strategy	<b>42</b>
<b>C</b>	Campaign Tactics Logic Model Template	<b>44</b>
<b>D</b>	Government	<b>45</b>
<b>E</b>	Youth, Parents & Educators	<b>47</b>
<b>F</b>	General Public	<b>51</b>
<b>G</b>	Business	<b>53</b>
<b>H</b>	Meeting Guidelines	<b>55</b>
<b>I</b>	Social Media	<b>56</b>
<b>J</b>	Infographics	<b>70</b>
<b>K</b>	Resources	<b>71</b>
<b>L</b>	Samples Messages from Stop.Think.Connect.	<b>76</b>

# Introduction

This toolkit is designed to provide governments or organizations guidance and resources for developing a cybersecurity awareness campaign.

Our goal is to help you think through your country's needs for a cybersecurity awareness campaign and how to best achieve it whether you have a large budget or limited resources. We want to help you build a campaign that is sustainable over a long period of time, educates your citizens and helps you build a national culture of cybersecurity.



# Background

We live in a digitally connected world. E-government, e-business, online banking, communication, and online healthcare are part of everyday life. Sensitive information, digital networks and critical infrastructure are all susceptible to cyber threats – from state sponsored attacks to organized crime to petty cybercrime. Everyone, from the highest government officials, business owners, the general public and children, is vulnerable to cybersecurity threats. It is no one person or entity's responsibility but rather a shared responsibility to prevent cybercrime. Government, businesses and private citizens all have a role to play in protecting the digital world. Government needs to protect critical infrastructure and confidential information, provide secure e-government portals, and protect numerous sensitive networks. Businesses need to protect intellectual property, financial information, networks, and customer and employee personal information. Individuals need to protect their personal finances and other information, along with protecting the safety of their children online. Because of the interconnected nature of the Internet, a weak link or breach in any of these systems can affect others. A data breach at one company can have far reaching effects. It can wreak havoc on the personal finances of individuals and also erode the national economic security of the country in which it happens. A piece of malware unwittingly downloaded onto a private citizen's device could make its way onto a government or corporate network if good policies for personal devices in the workplace are not in place.

The Internet reaches almost everyone in so many aspects of life; the audience is virtually everyone – children, families, educators, business, government, and the general public at large. Even if someone is not online, they are affected by cybersecurity because somewhere, someone else – a business, government, or somebody in their social circle – has personal information about them that is on a computer that is connected to the Internet. This brings focus on Cybercrime.

Cybercrimes are constituted by a vast range of different behaviors and techniques – including identity theft, child exploitation, cyberbullying, insider threats, phishing, spear phishing and many, many others – that needs to be addressed. Therefore although the audience for an awareness raising campaign is almost immeasurably large, you must take into account the fact that the message must be crafted depending on which specific sector of the audience you seek to reach. For example, a message that resonates with a CEO will not be the same message that resonates with a child or teacher and focus on the particular issues that are facing the country.

## The message must be attention grabbing, frequent and unified.

Educating people about cybersecurity is paramount to creating a culture of cybersecurity. Awareness is the first step towards developing a cyber-savvy citizenry. Raising awareness about cybersecurity and impacting behavior is no small undertaking. The marketplace for awareness campaigns is already crowded and people have limited bandwidth for more. The message must be attention grabbing, frequent and unified to cut through the constant barrage of advertisements, the 24-hour news cycle, and continuous stream of social media. It must be convincing and memorable. You are not seeking to sell widgets, but rather influence behavior.

You must appeal to the hearts and minds of your audience through messages that encourage them to take ownership of their own cybersecurity and in that way, become an ally in the fight against cybercrime.



# Instructions

Inside this toolkit you will find a 'how to do' cybersecurity awareness campaign planner, communication plans, sample messages, many online resources, examples of research, social media guidance and examples of metrics.

With the cybersecurity awareness campaign planner we seek to help you identify your goals and build a strategy to execute an awareness campaign. Along with the planner you will find, ideas, information and resources to help you implement your campaign. Many of the resources that are included are either free or low cost. The ideas and strategies that are included are also meant to help you make the most and best use of the resources that you have.

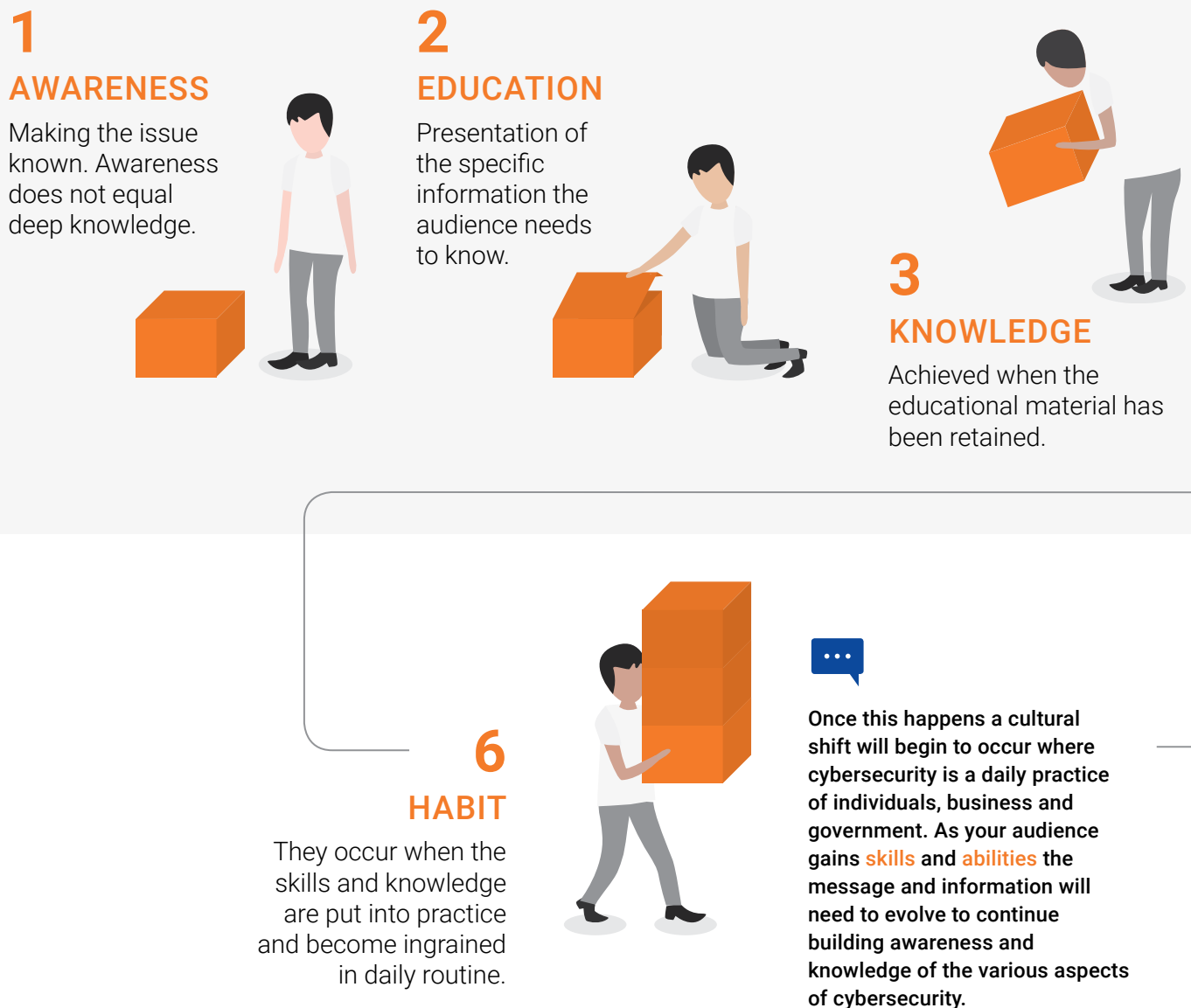
Read through the material. There is a wealth of information here for you. After you've read through the material and done your research, identify your stakeholder group (more about that on page 22) and get started. Hold a meeting of your stakeholder group to discuss the campaign. This meeting will likely take the better part of a day or more. Allow plenty of time for everyone to voice their opinion.

Following the meeting you should have a list of action items that you'll be able to identify. Hopefully this list will set you on your way to build your campaign, whether it's doing more research or beginning to put together a strategy executing your campaign.

This toolkit aims to provide the guidance needed to build a strategic cybersecurity awareness campaign. This is a complicated subject with no easy answers, but there is a way forward. By being strategic, understanding your audience, presenting them with a message that resonates and calls to action, and committing to a long-term campaign you will be able to effect change and develop a culture of cybersecurity.

# The Awareness & Education Continuum

As you start thinking about your goals for an awareness campaign and how to educate your audiences, it's important to distinguish between awareness and education. They are not the same thing. The process of building awareness can lead to education and eventually to behavior change. The following diagram shows the continuum for this process:





**Social change** of this nature takes a long time – a generation or more – to become fully integrated as a social norm, therefore realistic goals within stated timeframes should be set.

4

## SKILLS

Built upon the knowledge gained. They take practice and develop over time.



5

## ABILITY

Capacity to perform the skills required for proficiency.



The **first five steps** of the continuum may happen almost simultaneously or it may take a longer period of time depending on the success of the message, audience receptiveness and current level of knowledge.

**Constant repetition of the message** takes us to the sixth step, in which daily habits becomes ingrained to the point of being second nature.

7

## CULTURAL CHANGE

Built upon the knowledge gained. They take practice and develop over time.



# Campaign Structure

To ensure that the awareness and education continuum is achieved, a well-structured and planned campaign is necessary. Think about your campaign as a tiered structure; at the top tier is your campaign slogan and logo.

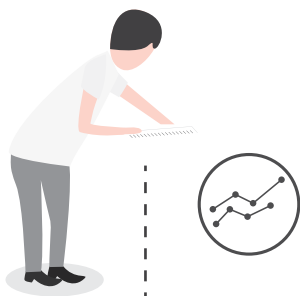


## Slogan and logo

The slogan is the short, pithy line that will, hopefully, be easily recognizable and set the tone for the campaign. The message and accompanying logo provide the identity for your campaign. Together, the slogan and logo are the brief message and graphic image that indicate to everyone “pay attention – there is something you need to know or think about.” These two items make up the campaign brand elements.

## Supporting message

The second tier of your campaign is the supporting messages. These messages begin to be more instructional in nature. Simple tips and advice are offered to the audience or provide direction on where to get more detailed information.



The slogan and logo are the cornerstone upon which you will build your campaign.



### 3

#### DETAILED INFORMATION

##### Website, programs, education materials

The third tier of the campaign is the educational part. This is where you offer detailed information whether it is instructions on how to create strong passwords and configure a firewall or a program on creating good cybersecurity workplace policies for CEO's.

#### RESEARCH & METRICS

##### This is the foundation of any campaign

**Data is of vital importance for understanding whether the messages and execution of the campaign is working.** As a result, research should be conducted at multiple stages of your campaign. Before you begin your campaign-planning look to see what data is available. Some things to know:

- How connected is your country?
- Where and how are people connecting to the Internet?
- Who is online?
- How is the Internet being used for business?
- What are the cybersecurity risks your country is facing?
- What are the economic losses from cyber threats?

Your government, Internet Service Providers (ISPs), Mobile carriers, software (security and otherwise), and Universities may already have some of this information. Develop partnerships with these institutions to gain access to the research that they may have to help further your campaign.

The metrics are the data that measure the success of your campaign. Gathering data before and during your campaign allows you to take a critical look at whether or not you are meeting your goals and helps you to evaluate the effectiveness of your campaign. This data can tell you if there's an area where you need to focus or if you need to possibly consider adjusting the message or changing tactics.

**K** See **Appendix K** for examples of research and surveys.

# The Message

At the very core, the message should be simple and easy for anyone to understand.

At the very core, the message should be simple and easy for anyone to understand. It's easy to fall into the trap of providing lots of highly technical information out of the desire to make your audience highly knowledgeable. Most of the people in your audiences don't need to be highly knowledgeable they mostly need to know how to protect themselves. Jumping into overly technical information will overwhelm. Just as counting is taught before addition, subtraction and

multiplication the approach for cybersecurity should be similar – teach the basics first. The message and accompanying educational material should be in plain language and strive to avoid technical jargon. Additional information (such as tips and advice) should be kept to a bare minimum to avoid overwhelming the audience with a list of too many things to remember. Advice should be framed in positive language and followed by actionable steps. Positive messages empower people to take

## For Example:

**Negative  
advice**



Computers that **don't have** up-to-date security software are at **risk for cybercrime**.

**Positive,  
action oriented**



**Help** thwart cybercrime by **keeping security** software up to date. Use the automatic update settings to **make it easy**.

**Negative  
advice**



Sharing **too much** personal information on social networking sites can lead to identity **theft**.

**Positive,  
action oriented**



**Be careful** with your personal information on social networks. **Review your privacy** settings and limit how much information you make available.

1. <http://stopthinkconnect.org/research-surveys/>




action and are more effective than those that are fear based. Research shows that cybersecurity<sup>1</sup> is no different. Fear based messages for cybersecurity result in people feeling powerless and that the situation is hopeless. Positive, empowering messages result in people feeling like they can affect the situation and that by taking action they are part of the solution.

The slogan and accompanying messages (and logo) should capture the attention of your audiences and move them to take action. The only way to know if you've accomplished this is through research. Your budget may dictate what type and how rigorous your research will be. The slogan and logo are the cornerstone upon which you will build your campaign. The messages that accompany them are vital elements. Research

into these items to ensure that they will resonate with your audience(s) is an investment in the success of your campaign.

A campaign of this sort is a commitment over time. The message needs to be consistent, persistent and flexible. As your audience becomes aware the message should evolve with them to bring them along in their knowledge of the issue and to address the evolutionary nature of cybersecurity.

The following table is a simple template to help you think through your messages, identify your audience, determine what your audiences needs to know and the key messages to achieve that goal.

Audience	What they need to know	Key Messages
 <p><b>General Public</b></p>	<ul style="list-style-type: none"> <li>• How to be secure online</li> <li>• How to protect their finances</li> <li>• How to protect their identity</li> <li>• What resources are available</li> <li>• Where to go for help</li> </ul>	<ul style="list-style-type: none"> <li>› Keep software up to date to help prevent cybercrime.</li> <li>› Protect your finances. Only use trusted, secure networks to access your financial information.</li> </ul>
 <p><b>Business</b></p>	<ul style="list-style-type: none"> <li>• How to protect their businesses</li> <li>• How to protect their finances</li> <li>• How to protect their data</li> <li>• How to educate their employees</li> <li>• What resources are available</li> <li>• Where to go for help</li> </ul>	<ul style="list-style-type: none"> <li>› Protect your business. Keep networks and data secure.</li> <li>› Know the risks. Educate yourself and your employees.</li> </ul>
 <p><b>Children</b></p>	<ul style="list-style-type: none"> <li>• How to be safe &amp; secure users of the Internet</li> <li>• How to protect their identity</li> <li>• What resources are available</li> <li>• Where to go for help</li> </ul>	<ul style="list-style-type: none"> <li>› Be a good cyber citizen. Be respectful and kind online.</li> <li>› Think before you post.</li> </ul>

**L** See Appendix L for a sample campaign plan.





# The Campaign Planner





## Stakeholders

Who needs to be part of the planning process?

- Government: Which agencies?
- Business
- Technology
- Financial Services
- Retails
- Community/ NGOs



## Goals

What do you want to achieve?

- Create a shift in attitudes and behavior
- Develop confident online citizens
- Reduce the incidence of cybercrime



## Audience

Who are you trying to impact?

- General Public
- Business
- Youth
- Educators
- Government



## Situation Analysis

What is your current situation?

- What do they already know?
- What do they need to know?
- What are the most important issues to be addressed?
- What resources (internal, capabilities, financial, existing platforms, partnerships) are available?
- What barriers to success need to be addressed?
- Is there anything that you don't want to see happen with the campaign?



## Strategy

How will you achieve your goal(s)?

- Develop Campaign Slogan and Message
- Build a strong web presence
- Deploy a set of targeted messages
- Develop outreach programs



## Tactics

What will you do to implement your strategy?

- Build a website
- Use social mediator to deliver messages on an ongoing basis
- Have a bi-weekly blog post
- Develop and disseminate posters across all government agencies
- Develop a K-12 classroom education program



## Success

How will it be measured?

### Outputs

- Media Coverage - Quantity
- Web & Media Reach (number of potential people)
- Events/Event attendance
- Collateral Disseminated
- Web visits

### Outcomes

- Media Coverage - Quality
- Brand Awareness
- Attitude Shift
- Behavior Changes

### Results

- Less Cybercrime
- More use of security software
- Cybersecurity budget inclusion
- Better cybercrime reporting
- Increased consumer confidence



# Stakeholders

## Who needs to be part of the planning process?

The very nature of cybersecurity is such that it is not “owned” by one entity or individual. Government, businesses (particularly Internet Service Providers, telecommunications, software and financial services), and individuals all have a responsibility in keeping a part of the Internet secure. Ideally an awareness campaign will be supported by a multitude of partners that can bring resources to bear – whether through direct funding, development of resources or inclusion in product or marketing materials.

All of these entities have a vested interest in creating a more secure cybersecurity environment and building consumer confidence in the online ecosystem. A partnership to deliver a unified message will be more effective than numerous disparate efforts, thereby increasing the chances for success. Buy-in of the campaign by Government, Business, Education and Community/Non-Governmental organizations will provide a broad platform to deliver the messages, reach many audiences and, hopefully, help provide the campaign with longevity.

Technology, financial and telecom industry leaders should participate as they are trusted resources in the marketplace and are the service providers for many of the online services that the general public and businesses rely on. They have an interest in building consumer confidence in the online marketplace and in protecting the networks and services they provide. Educating the public about how to be safer and more secure while using their services is a natural fit. As they are often in constant communication with the consumers, they have a natural platform to raise awareness and provide education. It makes sense for financial institutions to educate consumers about how safe online banking practices and for mobile carriers to provide information about mobile security. Providing a coordinated campaign with all actors strengthens the message for all.

Non-governmental organizations and community-based organizations are also natural partners. Through their respective missions to provide outreach and education to their audiences they can become great vehicles to

deliver educational programs, particularly to audiences that may otherwise be difficult to reach. They may also have particular insight into the specific needs of a population that could be valuable as you build your campaign and program.

Creating a cohort of these critical campaign stakeholders from the beginning will help build support and participation. Develop a list of who you think should be part of your stakeholder group. After you’ve identified your initial stakeholder group, invite them to participate in a facilitated discussion about the needs of the campaign. Including these people at the start of the campaign building process will help them have a sense of ownership over the campaign – which will increase the chances of participation later on. They may also make available valuable insight or resources such as research and distribution platforms.

The following sections will take you through a series of topics to consider. These sections are designed to assist you in gathering information from your stakeholders and this information will then form part of your strategy.

Allow for free flowing conversation around each topic. A neutral facilitator will help to remove bias and encourage all stakeholders to participate from their point of view.

**H** See **Appendix H** for meeting and facilitation guidelines.





# Goals

**What would success look like?**

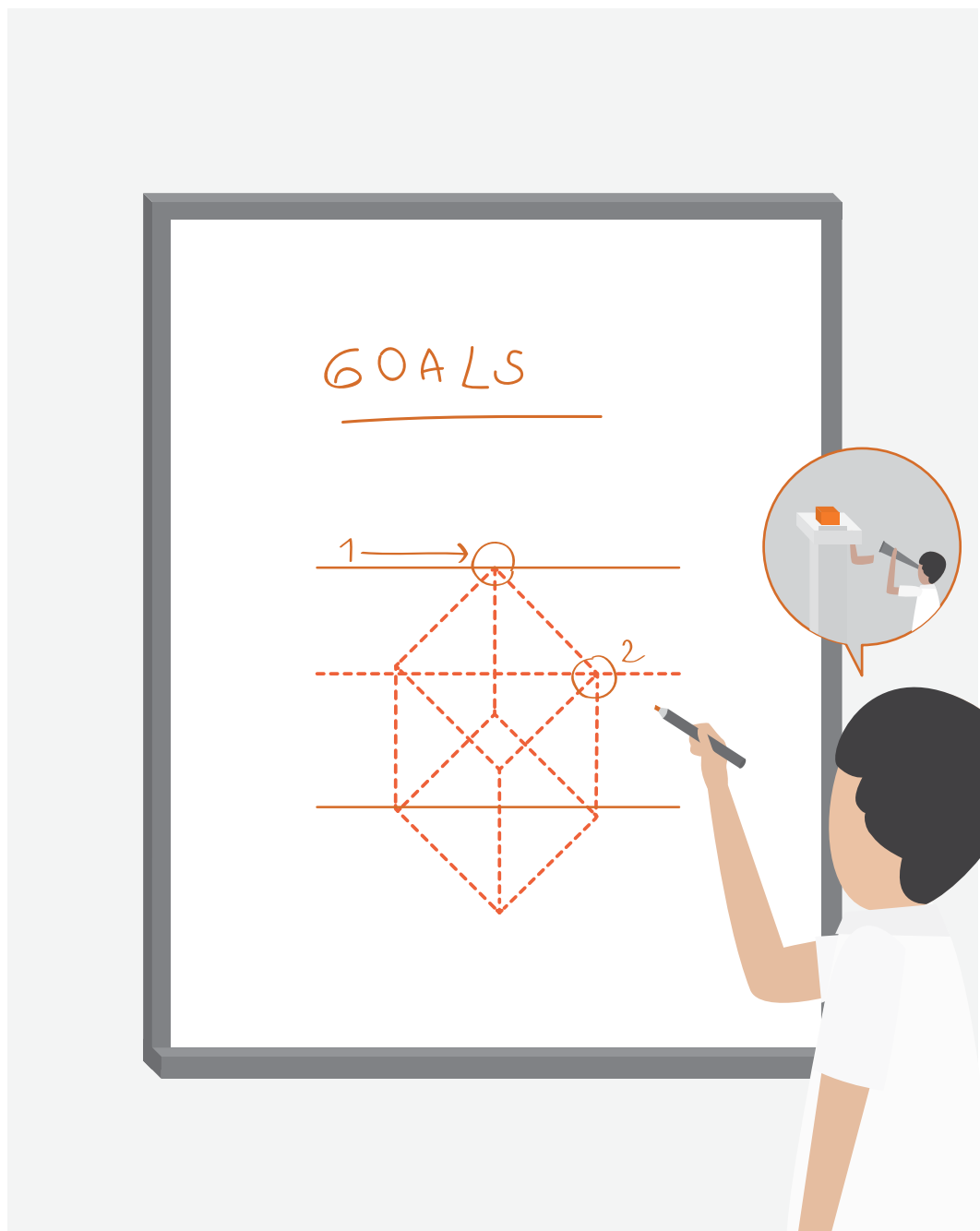
**What are the campaign objectives?**

Now that you have your critical stakeholder group gathered, the first part of your discussion should be about the need for a campaign and goals for a campaign. You will likely find that there are many goals that are quite varied.

## Some examples of success

---

- ✓ Risk-based behavioral/attitudinal changes
- ✓ Understanding the risks involved when adopting new technologies and implementing strategies to address them
- ✓ Less cybersecurity incidents
- ✓ User becoming so knowledgeable that they become carriers of the message. Transition from student to teacher
- ✓ Empower parents to facilitate responsible use of technology by children
- ✓ Improved protection of online intellectual property





# Audience

## Who is the campaign intended to reach?

This should be fairly straightforward. Who do you need to educate? It is likely that your group will come to the conclusion that everyone (the general public, businesses owners, employees, children) needs to be educated. Are there are specific groups that need special consideration (for example the elderly, non-native speakers, small business)? Is there a particular audience that is a higher priority than others?



### General Public

Cybersecurity affects everyone even those who aren't "online." Personal data is held by any number of entities, including government, business, large and small, healthcare providers and financial institutions. Email, social media, online shopping, online banking, at home and on the go, are becoming everyday activities for many people. All of this information and data is precious. Every time a breach occurs or an account is compromised trust in the Internet is eroded. Equipping people with the knowledge and skills to take be more cybersecure helps build confidence in the Internet marketplace and thwart cybercrime.

**F** See **Appendix F** for a sample campaign plan.



### Government

Although government may lead this campaign, government is also an audience for this campaign. Government collects and maintains all kinds of sensitive data that could prove detrimental to individuals, national security or the national economy if it were breached. Additionally sensitive networks that are vital to the running of the country can ill-afford to be put at risk. Government employees should be cyber-aware and understand their role in helping maintain a strong cybersecurity posture.

**D** See **Appendix D** for a sample campaign plan.



### Children

Children need to be educated about the safe and secure use of technology. Just as we teach them to navigate a city or town and learn the rules of the road, so too must they learn to navigate the digital world. Access to technology and the Internet abounds. Laptops at school (and often the requirement for using the Internet to complete or turn in an assignment), the use of mobile devices, all the ways in which we communicate, and how we share or gain access to information. The concerns are numerous – safety of the child, security of technology and information, and the ethics of use and communication. Education about the appropriate and responsible use of technology and the Internet should begin when a child begins to use them, which is often a very young age.

**E** See **Appendix E** for a sample campaign plan.





## Parents

Parents need to be educated along with their children. Often children know more about how to use the technology than their parents, which can lead to a feeling of helplessness and lead to avoidance of the issue. Arm parents with the information and resources they need to help guide their young people as they navigate the digital world. They may not know how to use all the technology but they can provide guidance and wisdom about how to make good decisions.

**E** See **Appendix E** for a sample campaign plan.



## Teachers

Teachers will be pivotal in educating children about all manner of online safety and security. Provide opportunities for them to learn, classroom materials and ongoing education. Programs covering basic online safety and security practices, cyberbullying, privacy, cybersecurity (viruses, hoaxes, fraud, etc.) and social media should be provided. As many of these issues can be quite complex, in-person training sessions to allow for in-depth discussion are advisable.

**E** See **Appendix E** for a sample campaign plan.



## Schools

Schools need to play a critical role in educating children about online safety and security. While most children have access to technology and the Internet, not all children will have parents or guardians with the knowledge and ability to provide good guidance about how to best navigate the digital world. Not only is there the social need for schools to help fill this roll, but there is also the expectation that children will use technology and the Internet to aid in their studies. Just as there are other classroom rules and expectations of safe and secure behavior, so to should there be for technology and the Internet. Moreover, as young people leave school and enter into University and the workplace there will be an expectation that they are savvy users of technology.

**E** See **Appendix E** for a sample campaign plan.



## Business

Businesses, whether large or small, should have a vested interest in cybersecurity. Intellectual property, finances, customer information and employee information are all sensitive data that can ill afford to be lost. That said, business can be a difficult audience to reach, particularly small to medium businesses who may not understand the gravity of the cybersecurity threat or whose owners and operators are completely immersed in the day-to-day operations of running a business. Educating business executives and workforce is also an opportunity to educate the general user as many of the steps employees should take in the workplace are the same as those security measures they should be implementing at home.

**G** See **Appendix G** for a sample campaign plan.



# Situation Analysis

## What is the current situation?

A good understanding of the state of the issue is paramount to developing and launching a successful campaign. It is important to ensure the situational analysis is done comprehensively.

Gather as much information ahead of this meeting as possible. An important part of the planning stage is to understand the local context. The questions below can help you paint a picture of what the cybersecurity threat profile looks like in your country. They will help provide context for why an awareness campaign is important and give credence to the requests for participation and funding. Your government, Internet Service Providers (ISPs), Mobile carriers, software (security, service provider, search), and Universities may already have some of this information. Other sources include:

**OAS**  
Organization  
of American States  
<http://www.oas.org/>

**ITU**  
The International  
Telecommunications  
Union  
<http://www.itu.int/>

**Pew Research Center**  
<http://www.pewglobal.org/>

**APWG**  
Anti-Phishing  
Working Group  
<http://www.antiphishing.org/>

A search through the media may also provide some intelligence, particularly regarding breaches to consumer facing businesses that impacted your country.

If you are unable to find relevant data for some of these questions, you may want to consider conducting some research depending on the resources you have available. Having a solid understanding of the cybersecurity landscape is important as you build your campaign. Therefore it is important to contact stakeholders that can assist in determining:

### FIND OUT

- How connected is your country?
- Where and how are people connecting to the Internet?
- Who is online?
- With what kind of devices?
- What kinds of operating systems and communications channels?
- For what kinds of products and services?
- How is the Internet being used for business?
- What is the scale of those businesses? (e.g., sole proprietorships? Agricultural cooperatives? SME for services? Light manufacturing?)
- What are the cybersecurity risks your country is facing?
- Why kinds of cybercrimes do you retail consumers face?
- What kind of cybercrimes to your businesses face?
- Are these cybercrimes distinguishable by cohort?
- What are the risks to your critical infrastructure?
- Have there been major breaches – either government or commercial – in the recent past?
- Are there threats of major breaches in the future?
- What are the economic losses or potential from cyber threats?

The questions below should help provide a framework of the problem. The next set of questions is meant to help you think more deeply about your campaign to determine your priorities and should be discussed with your stakeholder group:



### **What does the audience already know? What do they need to know?**

Don't assume knowledge or lack of knowledge. For example – you may assume that your audience doesn't know that they are supposed to use passwords. The real situation may be that the audience knows they are supposed to use passwords but they don't know how to create strong ones or manage them. Is there any existing research that can be used to help inform your campaign? Do you need to conduct more research to gain a better understanding of what your audience does and does not know?

### **What are the most important issues to be addressed?**

Are there particular cybersecurity issues that are of higher concern than others? Define your metric for prioritization: (e.g., Cost to business? Cost to people? Number affected by cybersecurity issues?)

### **What resources (internal capabilities, financial, existing platforms, partnerships) are available?**

### **What barriers to success need to be addressed?**

Are there any potential pitfalls that need to be avoided? Are there any issues specific to the sovereignty that need to be handled from the outset to ensure a successful campaign?

### **Is there anything that you don't want to see happen with the campaign?**

Think about other campaigns you've seen. What didn't you like about them? Where have those campaigns failed your country in ways you would want to avoid in the deployment of the nation's cybersecurity awareness program?

### **Given the resources that have been identified, the priority of issues and audiences to be addressed – what is a realistic goal for the start of this campaign? What are the top three priorities?**

In answering the above questions you should be able to identify what your objectives are with a campaign. You may find that there are short term and long term goals that can be articulated. Use the information from these questions to define your strategy and set your priorities for the campaign. It's possible that you will identify an area where research needs to be conducted in order to have a clear picture of the issue.

**K** See Appendix K for examples of some of the types of research and reports that have been conducted.



# Strategy

## How will you achieve your goal(s)?

Once you've identified your goals, including your top priorities, you need to determine: What will the campaign look like? Will there be public relations, a web presence, or outreach to the business community? Will there be ongoing research? What strategies will be used to deliver the campaign?

A strategy doesn't have to be a complex operation or design. A strategy should be a clear roadmap to achieve success. Be sure to include a timeline with your strategy to help set measurable benchmarks for the campaign. Example:



Your strategy will help you define the big picture. It provides the roadmap for the campaign and sets the high level objectives to keep you on track. A clearly defined strategy will also help you break down the campaign into realistic goals by prioritizing the work that needs to be done.

**A** See Appendix A for sample campaign strategies and **B** Appendix B for sample media relations strategies.





# Tactics

## What exactly will you do to implement your strategy?

Tactics are the details of your strategy. This is where you get into program specifics and detailed timelines. Think through each part of the strategy.

How will you achieve that goal? What activities need to take place?

What resources are needed? What is the timeframe for completion?

You should also establish how each activity will be measured. What strategies will be used to deliver the campaign?

**For Example:**

## Build a strong web presence

**Build and launch a consumer website within the first 3 months of the campaign**



- Establishment of website
- #Visitors
- # of Pages visited
- length of stay on page
- # downloads (content like posters, web banners, etc.)

**Use social media to deliver messages on an ongoing basis**

- Build Facebook page to engage young people
- Use Twitter for daily outreach
- Use Vine and YouTube to post short cybersecurity video



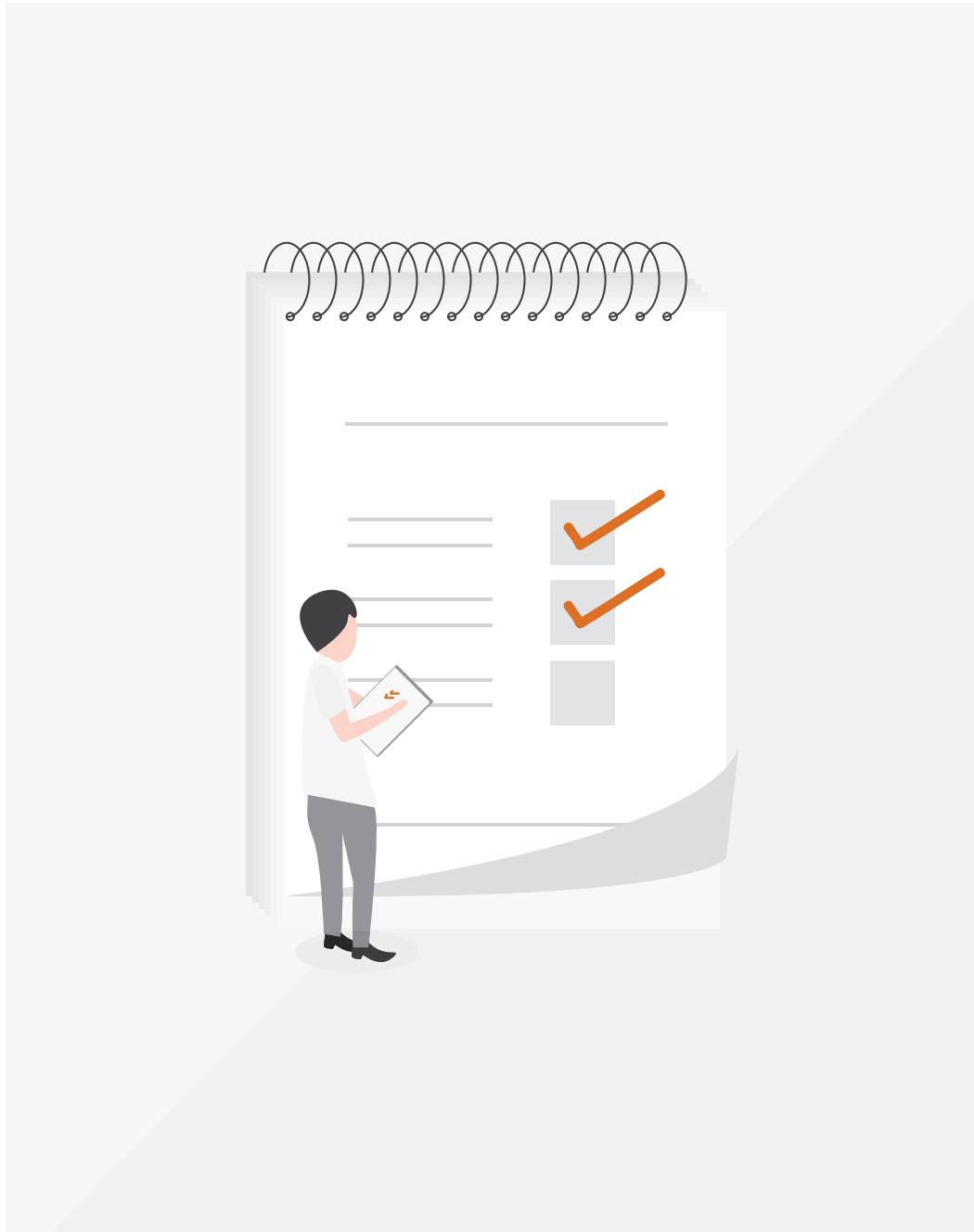
- Audience engagement: Number of followers, likes, views, retweets, shares (each social media platform has a way to measure audience participation)
- Number of posts

**Establish bi-weekly blog post by month 4 of campaign**

- Have a regular blogger or set of bloggers
- Use guest bloggers to round out content
- Establish an editorial calendar to provide



- Establishment of blog
- Number of blog posts
- Number of blog reposts (through social media, online news forums)
- Establishment of editorial calendar



# Goal 1

## Make Cybersecurity a Business Issue

### Objectives

- Cybersecurity becomes a C-Level issue
- Security becomes a business related issue and not just an IT issue: understanding why businesses should engage in secure practices
- Deliberate inclusion of funding for cybersecurity initiatives in budgets
- Improved protection of online intellectual property
- Risk-based behavioral attitudinal changes
- Understanding the risks involved when adopting new technologies and implementing strategies to address them

This campaign tactics logic model is designed to help you think through your tactics, the needed resources and what the outcomes and metrics will be.



See Appendix C for a template.

### ACTIVITIES

Things that will occur to achieve objectives

- Create an Executive Cybersecurity Roundtable
- Conduct Executive Briefings
- Develop & distribute business toolkit
- Media Relations
- Build website to house information

### INPUT/RESOURCES

Financial, technological, human

- Program Manager
- Funds for events and collateral development
- Funds for media relations
- Funding for website development
- Web manager

### OUTPUTS

Tangible, direct products of activities that lead to outcomes

- Roundtable Events
- Website launch
- Media Coverage
- CEO toolkit

### OUTCOMES

Desired results of activities

- CEOs more engaged on the issue
- Higher quality media coverage/placement
- Employees receive more education in the workplace

### MEASUREMENT

Indicators that can be measured

- Website/page visits
- Content downloads
- Increased spending on cybersecurity
- Cybersecurity included as budget line-item
- Media Coverage & Placement



## Goal 2

### Educate children about how to be safe and secure online

#### Objectives

- Children are educated about online safety & security



See Appendices I and J for guidance on Social Media and development of Infographics

<b>ACTIVITIES</b> <b>Things that will occur to achieve objectives</b>	<ul style="list-style-type: none"> <li>• Classroom education</li> <li>• Poster/Video Contest</li> <li>• Internet Safety &amp; Security Youth Council</li> <li>• Distribute information &amp; conduct outreach to families</li> <li>• Strategic partnerships with youth organizations</li> <li>• Build website to house information</li> <li>• Social Media</li> </ul>
<b>INPUT/RESOURCES</b> <b>Financial, technological, human</b>	<ul style="list-style-type: none"> <li>• Program Manager</li> <li>• Prizes for poster/video contest</li> <li>• Funds for events (youth council)</li> <li>• Funds for collateral development and distribution</li> <li>• Funds for website development</li> <li>• Web manager</li> </ul>
<b>OUTPUTS</b> <b>Tangible, direct products of activities that lead to outcomes</b>	<ul style="list-style-type: none"> <li>• Poster/Video contest</li> <li>• Establishment of Youth Council</li> <li>• Website launch</li> <li>• Collateral (posters, web banners) available on website</li> <li>• Create partnerships</li> </ul>
<b>OUTCOMES</b> <b>Desired results of activities</b>	<ul style="list-style-type: none"> <li>• Youth participate in contest</li> <li>• Launch of Youth Council</li> <li>• Young people more aware &amp; engaged on the issue</li> <li>• Strong partnerships with youth organizations</li> </ul>
<b>MEASUREMENT</b> <b>Indicators that can be measured</b>	<ul style="list-style-type: none"> <li>• Number of entries into contest</li> <li>• Higher awareness among children</li> <li>• Website/page visits</li> <li>• Content downloads</li> <li>• Facebook &amp; Twitter followers</li> <li>• Media coverage and placement</li> <li>• Number &amp; quality of partnerships</li> </ul>



# Success

## How will you know if you are successful?

Success was defined at the beginning of this exercise. Now that you've had deeper discussions about the issue and the elements of a successful campaign, how will you measure your success? Some of the ways success can be measured have already been discussed, but let's go a little deeper since this is a critical point. In order to know if you've met your goals, you must establish ways to measure success.

### There are two ways to measure success: quantitatively and qualitatively

**Quantitative data** is that which can be measured with a number. Number of visits to a website, number of articles written, number of people reached, time spent on a webpage, increase in spending, number of people with Internet access are all things that can be measured quantitatively.

**Qualitative data** is that which cannot be measured with a number. Attitude, feelings, tone, confidence are all things that are qualitative in nature. Quantitative data can

give you hard facts (example: there was a 25% increase in cybersecurity spending between 2014 and 2015 or there was a 18% increase in website visits from October to November) and can be used for large scale studies with statistical analysis. Qualitative data cannot be used for statistical analysis but can provide more insight as to how people feel or think. It is highly useful for small focus groups and to learn more about why people feel or behave a certain way.



## Outputs

(content & reach)

- Media Coverage - Quantity
- Web & Media Reach (number of potential people)
- Events/Event Attendance
- Collateral Disseminated
- Web visits
- Social sharing events  
(number of forwarded news items, etc.)
- Followers (On blogs, posts and Twitter accounts)
- Redirect events  
(301/302 status reports experienced by users, typically in spamming and phishing attacks)
- Malevolent communications  
(e.g., numbers of malware links delivered via SMS, email, fax and phishing messages delivered via SMS, email and fax)
- Abusive/unwanted communications  
(e.g., numbers of spam messages delivered, numbers of IVR and live-interview calls by phishers and scammers seeking to defraud)

## Outcomes

(Perceptions, knowledge, behaviour); Outcomes are the results of your outputs

- Media Coverage – Quality
- Brand Awareness
- Attitude Shift
- Behavior Changes

## Results

(Impact)

- Less cybercrime
- More use of security software
- Cybersecurity budget inclusion
- Better cybercrime reporting
- Increased consumer confidence

## There are different ways to gather these metrics

The measures that are directly related to your programming -such as social media, web site visits, media coverage, event participation, and collateral distribution- should be easy to establish and tracked on a monthly basis. They will give you an idea of how your program is ramping up and if you need to put more emphasis somewhere. In addition to articulating increases or reach, you can set goals for these metrics to help push your program forward:



Increase website visits by 10% each month



Increase followers on social media by 25% in the first quarter



Reach 25,000 followers on Twitter by the end of 2015



Host 8 events (or 2 events each quarter) by the end of the year

## Brand awareness

Brand awareness is another good indicator that your Campaign is on its way to success. **The best way to measure brand awareness is through marketing-style survey** where people are able to identify the campaign. A telephone or online platform is generally used for this type of research. **Generally 10-20 questions are asked.** This type of survey can also be useful to gather data on general cybersecurity awareness and practices. The downside of this type of data is that it is more qualitative in nature than quantitative as it relies on self-reporting. The upside is that it is possible to get a grasp on attitude towards cybersecurity and willingness to engage in better cybersecurity practices.

The other metrics that should be established are those that measure impact. **The measure of impact is the true testament of success for your campaign. Measuring the website visits and social media followers is an indication that you are headed in the right direction** and are reaching people but they don't measure whether your message created a change in behavior. This measurement will be more difficult as you will need to look at user behavior. Telephone/online surveys relying on self-reporting are one way to gather this information. Ability to monitor computer and network usage and interaction is the ideal way to gather this information, but would require access to an environment where that would be possible. A large business or another type of system such as a university could provide such a test environment.

### OTHER WAYS TO MEASURE IMPACT

Look at how businesses change their policies and procedures.

- Are they allocating more resources to cybersecurity? Have they put cybersecurity and privacy policies in place?
- Is there more or less reporting of cybercrime to law enforcement? What types of crime are being reported?
- Have financial institutions seen more secure behavior from their customers?
- Has there been a decrease or increase in phishing attacks?

This is a difficult area. Measuring user behavior on computers is tricky. You need to get creative and look to see what measurements you establish and continue to monitor.

The more baseline information you are able to establish at the beginning of your campaign, the better off your campaign will be. The metrics help you understand your campaign, whether you are on the right course or if you need to change tactics. The metrics will provide guidance and help you make decisions about your next steps in a rational manner.

# Putting it together

Now that you've gathered information, possibly conducted some research, established and met with a stakeholder group and explored the ins and outs of what you want to accomplish in establishing a campaign, it's time to bring the pieces together into a plan. But remember this is not a onetime event – your campaign must be repeatable, must be able to detect changes and adaptable to meet contemporary user needs.

Included in the appendix are examples of campaign strategies (A), media relations strategy (B), and audience specific strategies: Government (D), Youth, Parents & Educators (E), the General Public (F) and Business (G). Use these strategies for inspiration and ideas.

# Appendix

## A

## Campaign Strategies

A

B

C

D

E

F

G

H

I

J

K

L



### Media Relations

Continuous media relations is an important tactic to drive awareness of the campaign and provide information and education about cybersecurity issues to all audiences. Initiatives to work with the media to ensure that they understand cybersecurity issues and are providing the right information about how business and people can protect themselves should be pursued.



### Website

A single website for the campaign can house all of the materials for the campaign. A consolidated location will make content updates and collection of metrics, such as website visits and downloads of campaign materials, easier and more efficient.



### Social media

Facebook, Twitter, Vine and LinkedIn are all great venues for the campaign. Strategic positioning of the campaign through these channels is of key-importance to provide continuous outreach and engagement of audiences.



### Research and Data

Establish baseline cybersecurity profile for your country from existing research and new research and plan to conduct surveys and research on a regular basis (at least annually).



### Education Programs and Materials

Develop education programs designed for the specific needs of your individual audiences. A program to educate CEOs might consist of a CEO Roundtable forum, Cybersecurity for Business Guide and Toolkit for educating employees. A program for youth might include an education guide for parents, posters and videos for children, classroom lesson plans for teachers to deliver and posters to hang at home and school.



### Strategic partnerships

Develop strategic partnerships with business associations, faith based organizations, community based organizations and youth organizations. These partnerships will help deliver the campaign and engage various audiences.



### Events

Events can help bring focus and attention to the issue and are a great way to engage the desired audience. Various types of events for different audiences will be organized and hosted.





### Public Service Announcements (PSAs)

PSAs are a great way to reach your audiences and if done well can be used for years. PSAs should be kept positive in nature, use humor and always offer steps people can take towards protecting themselves. While TV broadcast quality PSAs can be expensive to develop, radio PSAs are relatively inexpensive to produce. Video PSAs for distribution via the Internet are also a great investment and can be done for significantly less cost than what is needed for television.



### Celebrity spokesperson

Celebrities can wield tremendous influence and power. Finding the right celebrity spokesperson(s) to participate in the campaign would be a huge win. Depending on budgets and passion for the cause this person(s) can be used in PSAs, events and media. (This particular tactic is a nice to have – not a need to have as it could be quite costly.)

A

B

C

D

E

F

G

H

I

J

K

L

## B

## Media Relations Strategies

A

B

C

D

E

F

G

H

I

J

K

L

A strong media relations strategy is of critical importance for this campaign. Local and national media can bring attention to cybersecurity as an issue for the general public, parents, teachers and the business community. It is of utmost importance that media get the story right. Just as all of the other audiences need to be educated about cybersecurity so too does the media. Your audiences will look to the media as a trusted source to provide vital information and timely coverage. Work with the media to ensure they understand cybersecurity issues and have good sources for comment and background information. A public relations professional should be retained (whether as an internal person working on the campaign or an outside agency) to do the media relations work for this campaign.



### Desired Outcomes

- Educated, well informed reporting
- In-depth cybersecurity coverage
- Increased reporting on cybersecurity issues



### Strategies and Tactics

#### Outreach: Educate the media

Make sure the media is telling the cybersecurity story. While an emphasis on technology media will be important, also conduct outreach to business, lifestyle, parenting and education media.

- How does cybersecurity affect your country?
- What concerns does government have?
- What concerns should citizens have?

- Why should businesses be concerned?
- What is the national security impact?
- What is the national economic impact?
- What are the basics steps to be more cyber secure?
- What are the potential problems and threats to be avoided?
- What should parents be teaching their children?

These are just a handful of the questions that the media should be addressing. After major breaches occur or a particular threat makes media headlines, offer up cybersecurity experts (from either the government or private sector) for comment to the media.

#### Fact Sheets

Media love facts and figures because they help to tell a better story. Provide fact sheets to the media about how cybersecurity impacts your country.

#### Infographics

In addition to helping to tell the story, infographics can (i) help drive media placement, (ii) be used on websites and social media, and (iii) be shared with partner organizations.

#### Personal stories

Moving from an abstract idea of a cyber threat (whether to a business or an individual) to an actual incident can help audiences connect and identify with the issue.

#### Quarterly Media Roundtable

Gather a small group of experts from government and the private sector to discuss cybersecurity with the media. Over the course of the year cover a broad array of topics: The cyber threat, impact on the critical infrastructure and economy, youth and cybersecurity, impact on the general public. Along with describing the threat(s), don't

forget to always include information on the steps that can be taken to increase security.

### Satellite and radio media tour

Launch the campaign with a media tour. Designate 1-2 experts (someone from government and someone from the private sector) to talk about the campaign, why cybersecurity awareness is important and a few simple steps people can take to start protecting themselves.



### Metrics

- Media coverage - quality and reach
- Fair and balanced reporting

A

B

C

D

E

F

G

H

I

J

K

L

# C

## Campaign tactics logic model template

A

B

**C**

D

E

F

G

H

I

J

K

L

### GOAL 1.

<b>ACTIVITIES</b> Things that will occur to achieve objectives	
<b>INPUT/ RESOURCES</b> Financial, technological, human	
<b>OUTPUTS</b> Tangible, direct products of activities that lead to outcomes	
<b>OUTCOMES</b> Desired results of activities	
<b>MEASUREMENT</b> Indicators that can be measured	

Objectives:

---

### GOAL 2.

<b>ACTIVITIES</b> Things that will occur to achieve objectives	
<b>INPUT/ RESOURCES</b> Financial, technological, human	
<b>OUTPUTS</b> Tangible, direct products of activities that lead to outcomes	
<b>OUTCOMES</b> Desired results of activities	
<b>MEASUREMENT</b> Indicators that can be measured	

Objectives:

---

## D

## Government

The following is a brief outline of a campaign strategy, tactics and metrics for a campaign with government employees as the audience.

Implement a government wide awareness and education campaign. As a major cybersecurity stakeholder and possibly leader of your campaign it will be important start with government as a major audience for the campaign. It will be a show of good faith to the public that Government takes cybersecurity seriously and is an adopter of good cyber practices. Primary adoption of the campaign will also prepare various ministries or departments to begin addressing the education and awareness needs of the private sector.

If not already in place, workplace cybersecurity, information sharing and privacy policies should be established and highlighted as part of the government wide awareness and education efforts.



### Desired Outcomes

- Parliament and Cabinet are educated about the actions to be taken in relation to cybersecurity (obtaining high-level/executive buy-in)
- Deliberate inclusion of funding for cybersecurity initiatives in budgets
- Improved protection of online intellectual property
- Greater collaboration between private and public sector (unified guidelines/strategies)
- Private-sector buy-in



### Strategies and Tactics

Government has three basic audiences that need to be addressed: executive, general employees and IT/IS employees. The entity designated with this responsibility should lead these efforts to ensure consistent messaging and distribution of materials. A government-wide campaign task force or council comprised of a designated person within each ministry might be helpful to help coordinate the activities and needs of all.

#### Executive

Support from the highest levels within each ministry is important to begin developing a culture of security. If cybersecurity best practices are not taken seriously and supported by the ministers and senior officials, then buy-in by employees would be more challenging. The opportunity to lead cultural change begins at the top.

Develop executive education materials to ensure that all ministers and senior officials understand the cyber threats, are taking the appropriate precautions and are supportive of the larger effort to educate all employees. Tactics to accomplish these goals include:

- Briefings
- Memos
- Monthly/weekly updates

#### General Employees

Create an ongoing campaign to educate employees. The messages should be geared towards best cybersecurity practices in the workplace, but also carry over to the home environment:

A

B

C

D

E

F

G

H

I

J

K

L

A

B

C

**D**

E

F

G

H

I

J

K

L

- *Website*
- Link to external campaign website
- Information on ministry websites/intranets

## • *Training sessions*

Provide quarterly or bi-annual in-person training sessions for all government employees. Reinforce the cybersecurity message with tips throughout the year via:

- *Computer screen saver/login messages (or campaign icon)*

- *Workplace signage*

- *Newsletter articles*

- *Blog posts*

- *Monthly brownbag/lunch discussions*

A wide variety of discussion subjects should be covered including work and personal or family related issues. Potential topics include:

- Securing the Workplace
- Privacy, Social Media and You
- Digital Kids: what parents should know
- The Internet of Things

## **Information Technology & Information Security Employees**

The IT/IS department should be a partner in educating all computer users. Proactive communication between IT/IS personnel and management is paramount to a good cybersecurity awareness program. An empowered IT team can be a great resource and ally in helping to educate the rest of the staff. IT/IS personnel should have access to continuing education programs to remain current on best cybersecurity practices. All ministries should seek to establish a positive relationship with people in these departments to allow for the flow of communication about current threats of which all employees should be wary (phishing and spear-phishing campaigns, malicious emails and websites, etc.).



## **Metrics**

- Website/page visits
- Participants in events (including in person and online)
- Training events and participants
- Reach of communications (blog posts, email, newsletters, memos)
- Cabinet and Parliament have been educated
- Funding for cybersecurity initiatives has been included in budgets
- Number of partnerships that have been established

## E

## Youth, Parents & Educators

The following is a brief outline of a campaign strategy, tactics and metrics for a campaign targeted to youth, parents and educators.



### Desired Outcomes

- Schools begin educating students about online safety and security
- Parents and teachers are empowered to facilitate responsible use of technology by children
- Teachers, parents and students become confident online citizens
- Users become so knowledgeable that they become carriers of the message



### Strategies and Tactics

#### Research

Conduct a survey to identify what teachers know about online safety and security and what is being taught in the classroom. Also conduct research on how young people use technology, what type of technology they have access to and what they know about online safety and security. Use this research as the basis for an annual survey to measure the effectiveness of the campaign and identify where teachers and young people need additional education.

#### Laptop Programs

If your country is conducting a one-to-one laptop program this is the perfect opportunity to provide education materials to students and parents. With each laptop include:

- Student safety and security guidelines and tip sheet
- Student “code of conduct” contract
- Parent online safety & security information guide (U.S. Federal Trade Commission guide is an excellent example of the type of material to include: [https://www.onguardonline.gov/articles/pdf-0001-netcetera\\_0.pdf](https://www.onguardonline.gov/articles/pdf-0001-netcetera_0.pdf))

#### Teachers

Teachers will be pivotal in educating children about all manner of online safety and security. Provide opportunities for them to learn, classroom materials and ongoing education. Programs covering basic online safety and security practices, cyberbullying, privacy, cybersecurity (viruses, hoaxes, fraud, etc.) and social media should be provided. As many of these issues can be quite complex, in-person training sessions to allow for in-depth discussion are advisable. Online resources through the Ministry or Department of Education should also be made available to provide teachers with information and tools to use in the classroom.

#### School

##### • School Assemblies

School assemblies are a great way to kick off the campaign in the school setting. They can happen any time of year however some dates to consider are start of school, Cybersecurity Awareness Month (October), Data Privacy Day (January 29), Internet Safety Day (February), and Internet Safety Month (June).

##### • Poster/Video Contest

Kids love contests. Harness their creative energy with a poster and/or video contest. This can be done at the school, district

A

B

C

D

E

F

G

H

I

J

K

L

A

B

C

D

E

F

G

H

I

J

K

L

and national level. Have the children use the National Cybersecurity Awareness Campaign tips as the basis for their creation. Give them rules and guidelines to follow (e.g., the poster or video must use the campaign slogan, the poster and or video must be positive in nature, the poster or video must contain at least one tip for how to stay safe and secure online).

## • *Ongoing Education – Classroom lessons*

Age appropriate classroom lessons should be taught as part of the general curriculum. Lessons can be tied to the use of the Internet and technology as they are used for other activities (for example going over the “rules of the road” before going online) or as stand alone lessons. Topics should include basic online safety and security, responsible use of technology, privacy, cyberbullying, social media, and cybersecurity. Classroom materials should include:

- Lesson plans and activities
- Posters
- Tip Sheets

## Parents

### • *Parent Forums*

Host parent forums throughout the year to discuss online safety and security topics. Gather a small panel of experts for a facilitated discussion. Invite experts from industry (telecom, ISPs, The Internet Society - ISOC), online safety, the school principal, and law enforcement. Make sure the forum is open and inviting of all types of questions. Have materials on hand to pass out afterwards (parent online safety & security guide, tip sheets, list of online resources). Topics can include: social media, cybersecurity, online safety and privacy, cybersecurity for the home, managing your child’s digital life. There are several points during the year that are natural to have a forum: start of school, Cybersecurity Awareness Month (October), Data Privacy Day (January 29), Internet Safety Day (February), and Internet Safety Month (June).

### • *Newsletter/Flyer*

Provide information on a regular basis via a school newsletter or other already existing form of communication (blog, website, social media). Or send a flyer home with

children periodically throughout the year with tips and reminders about online safety and security at home.

### • *Website*

Provide parent information and resources on campaign, school and Ministry of Education websites.

## Partnerships

Develop strategic partnerships with faith based organizations and community based organizations to strengthen youth outreach. Civil society programs and nonprofit organizations all provide opportunities to connect with children and young adults on the issue of cybersecurity and online safety. Engage these organizations to find out what types of issues they are seeing that are of particular concern and the types of materials and resources they would find the most helpful. Develop easy to use programs and activities designed specifically for use by these organizations (3-6 lesson plans for various age groups). Share campaign materials, provide speakers and request to participate in their conferences.

## Internet Safety & Security Youth Council

Establish a council to address cybersecurity and online safety concerns. The council should be comprised of a broad cross-section of people that are involved in the education system. This council will provide an opportunity for parents, students and school personnel to discuss the cybersecurity and online safety issues they are respectively concerned about and provide an opportunity to collaborate on programs and policies to implement in the school system.

- Ministry of Education
- Principals/School Leaders
- Teachers
- Parents
- Youth
- NGO’s
- Non-traditional education program leaders





## Celebrity spokesperson

Celebrities can wield tremendous influence and power. Engage a celebrity spokesperson that resonates with young people and can deliver an array of cybersecurity and online safety messages. This person can participate in events, PSA's and be a media spokesperson for the campaign. Any celebrity spokesperson should be managed by the Public Relations designee to ensure consistency of messaging. As this is potentially a high cost item, a celebrity spokesperson should be low on the priority list when deciding how to invest in the campaign if the budget is limited.

- Conduct Tweet chats on a monthly or quarterly basis to help drive the campaign message and engage an online audience in discussion about online safety and security issues. Topics to cover include cyberbullying, youth and appropriate use of technology (in and out of the classroom), and parenting a digital child. Invite partner organizations to be official partners in the Tweet Chat, thereby broadening the reach of the campaign and gain new followers.
- Distribute PSA's through traditional broadcast and print media. If budget allows, environmental advertising is a good method of distribution for PSA's as well.



## Metrics

- Website/page visits
- Content downloads
- Facebook & Twitter followers
- Number of Partnerships developed
- Participants in events (in person and online)
- Media coverage and placement
- Teachers trained
- Classroom programs implemented
- Materials distributed
- PSA distribution/reach



## Media

Focus on education, lifestyle and parenting media for pitching stories and offering up reactive interviews.

### • *Press Releases*

Release data, announce new programs and events

### • *Contributed Articles – Opinion-Editorials (op-ed)*

Offer up a monthly or weekly op-ed or article covering family online safety and security issues with an emphasis on children.



## Social Media

- Establish a weekly blog post to the website covering youth online safety and security issues. Develop a cadre of guest bloggers to cover various topics and help keep up the constant need for new content. An editorial calendar will help focus content but it's important to allow flexibility to allow for timely comment on current events.
- Use Twitter and Facebook to send out a stream of messages both proactive and reactive. Use these forums to cross-pollinate and establish a broad pool of experts and greater audience reach.

A

B

C

D

E

F

G

H

I

J

K

L

A

B

C

D

E

F

G

H

I

J

K

L

## Sample Youth Computer Code of Conduct

This code of conduct was written with a one-to-one laptop program in mind but could easily be used between parent/guardian and child or could easily be modified for general school computer use.

*I [FULL NAME] accept responsibility for this computer. As the individual responsible for this device, I agree to the following (initial each bullet point):*

- This computer has been entrusted to me and I am responsible for it.
- I will treat it with respect.
- I will use it for learning.
- I will not intentionally damage it or use it in a manner that could damage it.
- I will keep it in a safe and secure place.
- I will Practice Good Online Safety and Security Habits.
- I will Keep A Clean Machine. This means I will keep my operating system, security software, and web browsers up to date. If I don't know how to do this on my own I will have an adult help me.
- I will **Protect** My Personal Information.
- I will **not share** passwords.
- I will **be careful** about who and how I share personal information like my birthday, address, and phone number.
- I will **Connect with Care**. I will be careful about clicking on links, downloading content (videos, music, games).
- I will be a **Good Online Citizen**. What I do online can affect myself and others in positive or negative ways.
- I will **not post mean things or gossip about others**.
- I will **be an upstander** – someone who watches out for my friends and classmates.
- I will **not share** the personal information of others.
- I will be **respectful and considerate** of others.
- I will **Ask an Adult for Help** when I see something that is wrong or makes me uncomfortable.

Signed by  
[STUDENT SIGNATURE]

Date

### Parent or guardian

I have reviewed the code of conduct with [STUDENT'S NAME]. I agree to help my child follow this code of conduct and provide guidance where and when appropriate (or contact the teacher/school if I need assistance in providing guidance).

Signed by  
[PARENT/GUARDIAN SIGNATURE]

Date

## F

## General public

The following is a brief outline of a campaign strategy, tactics and metrics for a campaign for the general public.



### Desired Outcomes

- Confident online citizen
- Risk-based behavioral/attitudinal changes
- Understanding the risks involved when adopting new technologies and implementing strategies to address them
- Users become so knowledgeable that they become carriers of the message



### Research

Conduct broad research to gather a baseline of what people know about cybersecurity, how they are connecting to the Internet, how they are using the Internet and if they can identify the campaign. Use this research to serve as the start of an annual study with which to measure campaign progress and success.



### e-Government

Use all public facing government portals as an opportunity to educate the public. Place the campaign logo and one or two campaign tips in a banner on all portals or websites that the public access.



### Partnerships

Leverage existing partnerships and social programs with faith based organizations and community based organizations to strengthen outreach to the general public. Place an emphasis on those populations that can be difficult to reach and are often underserved such as the elderly and differently abled. Share campaign materials, provide speakers and request to participate in conferences of these organizations. Also engage these organizations to find out what types of issues they are seeing that are of particular concern that they may be able to help address and what types of materials and resources they would find the most helpful.



### Media

A strong media relations strategy is of critical importance for educating the public on cybersecurity issues. Local and national media can bring attention to the issue in general as well as focus on current threats and help make cybersecurity more relevant to the general public. A public relations professional should be retained (whether as an internal person working on the campaign or an outside agency) to do this work.

- Focus on general, pop culture, lifestyle, family media for pitching stories and offering up reactive interviews.
- Contributed Articles and op-ed  
Offer up a monthly or weekly op-ed or article covering a broad array of cybersecurity issues with an emphasis on protection of personal data and finances and the steps people should take to secure themselves against the various threats.

A

B

C

D

E

F

G

H

I

J

K

L

A

B

C

D

E

F

G

H

I

J

K

L



## Social Media

- Establish a weekly blog post to the website. Develop a cadre of guest bloggers to cover various topics and help keep up the constant need for new content. An editorial calendar will help focus content but it's important to allow flexibility to allow for timely comment on current events.
- Use Twitter and Facebook to send out a constant drumbeat of messages – both proactive and reactive. Use these forums to cross-pollinate and establish a broad pool of experts and greater audience reach.
- Conduct Tweet chats on a quarterly basis to help drive the campaign message and engage an online audience in discussion cybersecurity issues. Topics to cover include: understanding the threat, the Internet of things, mobile cybersecurity, and family cybersecurity. Invite partner organizations to be official partners in the Tweet chat, thereby broadening the reach of the campaign and gain new followers.
- Distribute PSA's through broadcast and print media. Environmental media (billboards, bus posters, etc.) are also a good way to disseminate PSA's.



## Metrics

- Website/page visits
- Content downloads
- Facebook & Twitter followers
- Number of Partnerships developed
- Participants in events (including in person and online)
- Media coverage and placement
- PSA distribution

# G

## Business

The following is a brief outline of a campaign strategy, tactics and metrics for a campaign for business.



### Desired Outcomes

- Cybersecurity becomes a C-Level issue
- Security becomes a business-related issue and not just an IT issue: understanding why businesses should engage in secure practices
- Deliberate inclusion of funding for cybersecurity initiatives in budgets
- Improved protection of online intellectual property
- Risk-based behavioral/attitudinal changes
- Understanding the risks involved when adopting new technologies and implementing strategies to address them



### Research

Conduct surveys to assess the cybersecurity preparedness of businesses and their employees. Separate surveys for small businesses and larger enterprises should be done as different resources (financial, number of employees and organizational structure) dictate the approach to cybersecurity. Use these surveys as the basis for ongoing annual benchmark surveys to measure the effectiveness of the campaign.



### Cybersecurity for Business Toolkit

Business owners are busy people. A simple toolkit with resources to educate themselves, their employees and begin improving their cybersecurity practices can go a long ways towards engaging business owners on this topic. In the toolkit provide:

- Fact sheet
- A list of easy to implement steps to immediately improve their cybersecurity posture
- Resource list
- Workplace posters
- Web banners
- Employee education guide
- Sample CEO letter to employees
- Sample workplace cybersecurity policy to potentially include topics such as:
  - Mobile use
  - Information sharing
  - Social media use
  - Bring your own device (BYOD)



### Partnerships

Build strategic partnerships with business and industry organizations (such as Rotary Club, Manufacturer's Associations, Trade Associations, Human Resource Management Associations, and Business Networks). Use these organizations that businesses owners are already participating with as a means to help disseminate cybersecurity information. Provide a campaign toolkit that includes materials such as information about the campaign, draft email (to their constituents), talking points, graphics, posters, web banners, business toolkit and web resources. Offer up monthly or quarterly blog posts and regular newsletter articles.

A

B

C

D

E

F

G

H

I

J

K

L

A

B

C

D

E

F

**G**

H

I

J

K

L



## Business Cybersecurity Security Executive Roundtables

Host a cybersecurity roundtable series targeted specifically at executives, owners and operators 4 – 6 times over the course of the year. Partner with organizations such as Internet societies, computer societies (ISC(2), APWG, ISOC), and Universities to provide security expert advice for small, medium and large businesses. Provide information about the threats, stories from businesses that have been affected by cybersecurity threats and information about what steps businesses can take to protect themselves. Potential topics include:

- Managing a Healthy Network
- Privacy 101
- Cybersecurity: The Basics
- Educating your Workforce
- Bring Your Own Device: Policy
- The Threat Landscape
- Cybersecurity: It's your business
- Insider Threats



## Cybersecurity Speakers Bureau

Target business organizations for speaking opportunities. Offer up speakers to monthly meetings and annual conferences. Discuss how Internet security impacts business and provide resources (website, brochures, follow-up discussion opportunities) for businesses to learn more.



## Media

- Focus on general, business papers and magazines, and industry trade newsletters for pitching stories and offering up reactive interviews.
  - Contributed Articles – Op-Eds
- Offer up an executive focused monthly or weekly op-ed or article covering a broad array of business cybersecurity issues –

workplace policies, bring your own device (BYOD), insider threats, building a culture of cybersecurity.



## Social Media

- Establish a weekly business focused blog post to the website. Develop a cadre of guest bloggers to cover various topics and help keep up the constant need for new content. An editorial calendar will help focus content but it's important to allow flexibility to allow for timely comment on current events.
- Use Twitter, Facebook and LinkedIn to send out a constant drumbeat of messages – both proactive and reactive. Use these forums to cross-pollinate and establish a broad pool of experts and greater audience reach.
- Conduct Tweet chats on a quarterly basis to help drive the campaign message and engage an online audience in discussion cybersecurity issues. Topics to cover include: understanding the threat, the Internet of things, BYOD, and cybersecurity & privacy best practices. Invite partner organizations to be official partners in the Tweet Chat, thereby broadening the reach of the campaign and gain new followers.



## Metrics

- Website/page visits
- Content downloads
- Facebook, Twitter and LinkedIn followers
- Number of Partnerships developed
- Participants in events (including in person and online)
- Media coverage and placement

## Meeting guidelines

### Meeting & Facilitation Guide

The following guidelines are to provide a framework for a facilitated discussion.

- *Use a Facilitator and a note taker*
  - The person leading or facilitating the discussion should be able to maintain a neutral stance on the topic under discussion. It may be helpful to have someone without a vested interest in the outcome of the discussion to be the facilitator.
  - The role of the facilitator is to guide the conversation in such a way that everyone participating has an opportunity to be heard. This person should also be able to, if need be, referee, refocus and move the meeting along.
  - The note taker should be a different person to allow the facilitator to focus on conducting the meeting.
- *Have a clear purpose and agenda for the meeting*
  - Provide an agenda with a clearly articulated set of objectives for the meeting. It's important that the meeting participants understand what the goals of the meeting are so they can be prepared. Send the meeting agenda and any reports or reading well in advance so that everyone has an opportunity to prepare.
- *Set Ground Rules for the Meeting*
  - It's important that everyone understand the manner in which the meeting will be conducted and agree to a set of rules.
  - Listen respectfully without interrupting
  - Respect other's point of view
  - Allow everyone the chance to speak
  - Criticize ideas, not people
- *Educate the Participants*

You may have people from different areas of expertise or with different levels of knowledge about the issue. Provide advanced reading material, but also take some time at the beginning of the meeting (or as you switch topics) to educate your meeting participants about the topic at hand to help create a common basis of understanding. For example, at the start of the meeting have an expert conduct a presentation on cybersecurity and the impact on your country or, as you discuss awareness campaigns, have a public relations (PR) professional give a presentation on elements of a successful awareness campaign.

A

B

C

D

E

F

G

H

I

J

K

L

## Social media

Social media is a fantastic, low cost way to reach an audience. Facebook, Twitter and LinkedIn are all platforms that you should consider for your campaign. These channels allow you to be in constant contact with your audience, gain a large following quickly, build a community interested in cybersecurity, provide an opportunity to address issues in real time, position yourself as a thought leader, and respond to questions your audience may have in a community forum. There's no good reason to not use social media!

### Social Media Tips

Building an engaging social media network can be a daunting task. Here are a few tips to build your network and engage your audience in a meaningful way.

- *Have great content*

Social media isn't just about selling your idea or issue; it's about providing good content for your audience to consume. In addition to developing your own content (website material, blog posts, tips sheets, infographics, news releases and media mentions) make it a habit to regularly share relevant content of others (whether it's a government agency, corporation, news article or private citizen). You'll be more relevant and gain more followers.

- *Build your network*

After you've established your social media site, actively invite people to join your network. "Like" other organizations' pages and feeds that are relevant to cybersecurity and online safety. Other organizations are more likely to "like" and follow your site or feed if you are willing to support their site.

- *Engage your audience in conversation*

Ask questions on your site or feed. Allow people to answer back. Let your followers to

post questions and comments and be sure to respond to them.

- *Be persistent and post often*

It will take time to build your social network. Posting good content often (2-3 times per day to start) will help you build your network and provide a reason for your followers to keep coming back.

- *Use graphics and videos*

Photos, graphics and videos make for great content that will garner a lot of likes and comments.

- *Cross Promote*

Cross pollinate your social media sites. Connect with your website (blog posts), Facebook, Twitter, LinkedIn, and Instagram.

- *Support your followers and partner organizations*

Give a shout out to your partner organizations when they announce new initiatives, are in the news or post good content.

- *Use Hashtags*

Hashtags (#stopthinkconnect, #stopcyberbullying, #dataprivacyday) create searchable links and help organize content and discussions. (Here are a couple of resources that give a good, more in-depth primer on hashtags: <https://support.twitter.com/articles/49309-using-hashtags-on-twitter> and <http://mashable.com/2013/10/08/what-is-hashtag/>)



### Twitter Chats

**By Emily Eckland, Digital Strategist**

Twitter Chats are a great way to engage



your online audiences. They are basically a planned, facilitated online discussion. You pick the time and topic, invite a few experts to join you, and then advertise to your social media universe that you will be having this discussion. The following is an overview of Frequently Asked Questions (FAQ) about Twitter chats followed by a couple of examples of how to plan one.

### What is a Twitter chat?

**What:** A Twitter chat is an online discussion that takes place over Twitter and is organized via a designated hashtag (#). Examples of hashtags are: #onlinesafety, #election, #puppies.

**How:** People follow the chat by searching for the designated hashtag. In order to participate in the chat, each tweet must also include the designated hashtag. There are websites and tools you can use to create a “virtual chat room” and organize your Twitter feeds.

**Who:** Anyone can participate in a Twitter chat. There are typically hosts or moderators and official chat participants, but anyone is welcome to join the discussion. Of course, you also need a Twitter account and handle (name, such as @\_\_\_\_\_) to participate.

**Why:** Twitter chats are a great, free, and relatively easy way to connect with people, increase brand awareness and get a message across on a social platform.

### Other Frequently Asked Questions:

#### How do I come up with the hashtag for my chat?

The hashtag is entirely your choice, but it is helpful to have the word “chat” or “talk” in it to signify that it is a Twitter chat, and not just a hashtag. (Examples: #TechTalk, #SafetyChat). You may also think about using your organization’s name or an acronym to build brand identity. (For example, if your organization is the Association of Cat Lovers, you may want to use #ACLChat for the hashtag.) It’s also a good idea to see if the hashtag you plan to use is being used by another organization. You can do this by searching the hashtag on Twitter and looking for any results.

#### How long are Twitter chats?

Twitter is a fast-moving, fluid platform and chats go by very quickly. Most Twitter chats are typically an hour or one hour, 30 minutes. It would be challenging to hold a Twitter chat in 30 minutes.

#### How should I format my Twitter chat?

A big part of Twitter chats is engaging with your “audience.” Twitter chats can be formatted in several different ways, but the most popular ones ask their panelists a series of questions and then allow time for the “audience” to ask questions of their guests. You could also hold a chat without panelists and pose your questions to everyone participating in the chat.

You should start each chat with a few introductory tweets that go over the topic and allow you and your panelists to introduce yourselves to your “audience.” After that, the moderator can start asking questions. For an hour-long chat with 3-5 panelists, 8-10 questions is typically enough to get through and leave time for audience questions. It can take 3-5 minutes for everyone to answer a question too. It’s helpful to have a few extra questions you can use if you have more time to spare. A tweet is 140 characters, which isn’t a lot of space to get my message across. What if I need to say more? Don’t feel pressured to try and fit everything you’re trying to say in 140 characters! You can use multiple tweets to answer a question (just make sure to include the hashtag!). It’s a good idea to write out your responses beforehand and have a list of handy URLs or messages that you want to get across during the chat.

#### Twitter seems like a bit of a free for all. Is there any way to create a more orderly chat?

You will have people tweeting at the same time so your responses may not appear consecutively; this is just the nature of Twitter. But there are some ways to control the flow of the chat, such as creating a tweeting order for your panelists. It’s also helpful for everyone to label questions and answers. (For example: Q1, A1, etc.)



A

B

C

D

E

F

G

H

I

J

K

L

### Do I need to be in the same room as my Twitter chat participants?

No, and that's the beauty of social media! At any given chat, you could have participants from across the globe in several different time zones. However, you can set up a conference telephone line to use for the chat. Some people use a conference line to establish a tweeting order for panelists, or to help address any audience questions, and for general troubleshooting.

### How and when should I promote my Twitter chat?

You can promote the chat however you'd like, but it's a good idea to have a point of reference for people to see all of the details about your chat. This can be a page on your website, a listing on an events website like Eventbrite, or even another social media account like Facebook, LinkedIn and Google+. It's a good idea to promote the chat in as many ways as possible: Email, e-newsletters, social media (including Facebook, LinkedIn, Google+), on your website, etc.

Since Twitter is so fluid, you can promote the chat at any time. But most people start to promote a week and more heavily in the days leading up to the chat. You can also take advantage of tools like HootSuite, TweetDeck and others to schedule promotional tweets in advance.

### What does RT and MT mean?

RT is short for re-tweet and appears on Twitter and other platforms as an icon with two arrows. You can RT (essentially, copying what a Twitter handle posted and making it available to your followers) by hitting the icon on Twitter or by creating a new message, copying the message you want to retweet and typing "RT @(Twitter handle you are retweeting)" beforehand. MT is short for modified tweet, which is a tweet you want to RT and add your own message before posting. Many times, an original tweet plus your own message in front of it will cause it to be more than 140 characters, so you will have to edit it before posting.

### RT Example

Original Tweet: @HappyFeet: I love to dance and it makes me so happy.

RT Tweet. @LoveDancing: Me too! What is your favorite dance move? RT@HappyFeet: I love to dance and it makes me so happy.

### MT Example

Original Tweet: @BurgerLover: The best hamburger toppings of all time are fried eggs, avocado, bacon, cheese – preferably smoked gouda. #burgers #feedme.

MT Tweet: @PattiesnBuns: You forgot pickles, sautéed onion! MT@BurgerLover: The best hamburger toppings of all time are fried eggs, avocado, bacon, cheese.

### Are there ways to track the success of my chats?

Yes, there are several free services like: Topsy, Tweetchup, and Buffer. There are also other analytics services that are subscription-based, like SimplyMeasured, Crowdbooster, and Twitonomy. If you use a URL shortener like Bit.ly, you can also track how many clicks your tweets with bit.lys received by checking your account.

### What other best practices should I know about?

Feel free to re-tweet (RT) responses that you like from other participants. And add a hashtag (#) to common keywords, because it will allow them to be searchable on Twitter and allow for wider visibility.



### Examples of Twitter Chat Scripts

#### Script# 1: Online Safety at Home Twitter Chat

Mock information, including the moderator questions and responses from one panelist.

#### Online Safety at Home #CyberSafeChat Twitter Chat [INSERT DATE, TIME, ETC.]

Brand	Organizations	Twitter Handles	Organization Website/ Other Social Media
Theme / Hashtags	General Online Safety Join _____ as we discuss _____. Learn _____, _____ and _____ at this chat.		
Panelists	Moderator: @Moderator Panelists: @Panelist1		

#### Promotional Tweets to Send Out Before and During the Chat

Twitter

Join \_\_, \_\_\_\_, \_\_ for a #Twitter chat \_\_ at \_\_. Use #\_\_ to join!

Learn \_\_\_\_\_ at our \_\_\_\_\_ #Twitter chat on \_\_\_\_\_ at \_\_. Use #\_\_ to join!

Brand on Facebook

Like us on #Facebook for more:

Brand on Twitter

Stay connected after our #Twitter Chat by following \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_

Additional Info

Stay informed and get \_\_\_\_\_ tips here:

#### Welcome and Intro Tweets

2:50 p.m. ET

Only 10 more minutes until our \_\_\_\_\_ # Twitter Chat!  
We hope you'll join us! Use \_\_\_\_\_ to join!

3:00 p.m. ET  
INTRO

@Moderator: Welcome to our #onlinesafety #Twitter chat!  
#CyberSafeChat



A

B

C

D

E

F

G

H

I

J

K

L

# Appendix

- A
- B
- C
- D
- E
- F
- G
- H
- I**
- J
- K
- L

3:00 p.m. ET  
INTRO

@Moderator: Today we'll be talking about ways you and your family can stay safe #online. #CyberSafeChat

@Moderator: Our guests are \_\_\_\_\_ #CyberSafeChat

@Moderator: Let's have them introduce themselves! #CyberSafeChat

@Panelist1: Hi! We are \_\_\_\_ and our mission is \_\_\_\_\_. #CyberSafeChat

@Panelist1: We're thrilled to be a part of these series of this #Twitter chat & happy to help empower people with resources to stay safer online. #CyberSafeChat

*(Allow other panelists to introduce themselves.)*

@Moderator: Great! Who else do we have joining us for our #CyberSafeChat today?

*(Moderator should acknowledge and welcome some people who respond to this tweet.)*

3:05 p.m. ET  
QUESTION 1

Moderator: Great! Let's begin. We're going to start off with a broad, but important question today. #CyberSafeChat

Moderator: Q1: What are 3 simple things we can do to stay #safe and #secure online every day? #CyberSafeChat

@Panelist1: A1 1) Make sure all of your devices have the latest #software, OS, anti-virus, web browsers and apps. #CyberSafeChat

@Panelist1: A1 2) Don't click on suspicious URLs or emails When in doubt, throw it out! #CyberSafeChat

@Panelist1: A1 3) Be careful using public, unsecured #WiFi. Don't bank, shop, or enter personal information #online. #CyberSafeChat

*(Wait about 3 minutes for people to respond and moderator/panelists can RT the best responses/call out good responses from participants)*

3:10 p.m. ET  
QUESTION 2

@Moderator: Wow! These were some fantastic responses! Thank to you everyone for sharing these great tips. #CyberSafeChat

@Moderator: @Panelist1 & others brought up a good point about clicking on suspicious links. #CyberSafeChat

@Moderator: Q2 What are some ways to spot scams & potential #phishing attacks? #CyberSafeChat

3:14 p.m. ET  
QUESTION 3

@Panelist1: A2: Be wary of emails that ask for personal information or ask you to act quickly. Typos and misspelling are clues, too. #CyberSafeChat

@Panelist1: A2: Remember, if something sounds too good to be true, it probably is! #CyberSafeChat

*(RT the best responses/call out good responses from participants)*

@Moderator: Let's switch gears a bit and move onto another important aspect: #onlinesafety & families. #CyberSafeChat

@Moderator: Many kids have their own #mobile devices & computers, so the concept of a computer in the family room may not be valid. #CyberSafeChat

@Moderator: Q3: Are there any critical things that #parents should enforce when their #kids are #online? #CyberSafeChat

@Panelist1: A3 Help kids identify safe, credible sites & be cautious about clicking on, downloading & posting content. #CyberSafeChat

@Panelist1: A3 Know the protection & #privacy features of your #devices & the websites & #apps your children use. Your ISP can help, too. #CyberSafeChat

*(RT the best responses/call out good responses from participants)*

3:14 p.m. ET  
QUESTION 3

@Moderator: Speaking of going #online at home – our next question may sound basic, but it's still good for everyone to know! #CyberSafeChat

@Moderator: Q4: How can you ensure your home #WiFi network is secure? #CyberSafeChat

@Panelist1: A4: Make sure your router is WPA2 or WPA-PSAK, which have stronger authentication/encryption. WEP isn't as secure. #CyberSafeChat

@Panelist1: A4: Change the SSID (name) on the router but don't use personal ones, like "Ann's WIFI." Use mix of numbers/letters. #CyberSafeChat

@Panelist1: A4: Change the password & make it strong & long – using a mix of upper/lowercase letters & numbers & symbols. #CyberSafeChat

*(RT the best responses/call out good responses from participants)*

3:22 p.m. ET  
QUESTION 5

@Moderator: Okay, time to switch things up a bit. Our next question is a "true or false." #CyberSafeChat

@Moderator: Q5: True or false: All #Internet-enabled #devices need anti-virus protection? #CyberSafeChat

@Panelist1: A5: True! Phones, tablets & other devices are vulnerable to threats. You should protect them like you would your computer. #CyberSafeChat

*(RT the best responses/call out good responses from participants)*

3:26 p.m. ET  
QUESTION 6

@Moderator: Q6: What are the most important things to remember to stay safe online on #mobile devices? #CyberSafeChat

@Panelist1: A6: Read the #privacy policy & know what info an app collects (contacts, photos, location) before you download! #CyberSafeChat

*(RT the best responses/call out good responses from participants)*

3:30 p.m. ET  
QUESTION 7

@Moderator: We're going to move on to another basic, but extremely important topic: #passwords. #CyberSafeChat

@Moderator: Q7: What are the elements of a good #password & are there other technologies that make it more secure? #CyberSafeChat

@Panelist1: A7: Elements of a good password: Long & strong with a mix of upper/lowercase letters, numbers and symbols #CyberSafeChat

@Panelist1: A7: Ex: @\$!llygRAY3l3ph@^t is more secure than "asillygrayelephant." #CyberSafeChat

@Panelist1: A7: Many websites offer protection beyond the password, like 2 step authentication - a better way to secure #online accounts. #CyberSafeChat

*(RT the best responses/call out good responses from participants)*

3:34 p.m. ET  
QUESTION 8

@Moderator: We touched upon this earlier, but let's revisit the notion of using public #WiFi safely. #CyberSafeChat

@Moderator: Q8: How do you detect unsecured #WiFi & what websites should you avoid while using it?

@Panelist1: A8: Unsecured #WiFi doesn't require you to type a password before you access it. #CyberSafeChat

@Panelist1: A8: Free #WiFi in coffee shops, airports, hotels, etc. is usually unsecure. #CyberSafeChat

<p>3:38 p.m. ET QUESTION 9</p>	<p>@Panelist1: A8: If using unsecure #WiFi, you shouldn't visit websites that require you to type your username &amp; password. #CyberSafeChat</p> <p>.....</p> <p>@Panelist1: A8: Examples of this are email, social networks, travel websites. And never enter credit card or financial info. #CyberSafeChat</p> <p>.....</p> <p><i>(RT the best responses/call out good responses from participants)</i></p>
<p>3:42 p.m. ET QUESTION 10</p>	<p>@Moderator: This next question is about something that most people are concerned about: #cybercrime #CyberSafeChat</p> <p>.....</p> <p>@Moderator: Q9: If you discover you're a victim of #cybercrime, where should you report it &amp; turn for help? #CyberSafeChat</p> <p>.....</p> <p>@Panelist1: Q9: Notify your local law enforcement agency &amp; the #Internet Crime Complaint Center: <a href="http://www.ic3.gov/default.aspx">http://www.ic3.gov/default.aspx</a>. #CyberSafeChat</p> <p>.....</p> <p>@Panelist1: Q9: If you're a victim of #idtheft, notify your financial institutions immediately &amp; contact the credit bureaus. #CyberSafeChat</p> <p>.....</p> <p>@Panelist1: Q9: Collect &amp; keep any evidence (credit card statements, emails, etc.), change passwords &amp; update your devices. #CyberSafeChat</p> <p>.....</p> <p><i>(RT the best responses/call out good responses from participants)</i></p>
<p>3:45 p.m. ET</p>	<p>@Moderator: We have time for one last question before we turn it over to our audience.... #CyberSafeChat</p> <p>.....</p> <p>@Moderator: Q10: What #onlinesafety resources do you recommend for people who want to #protect themselves &amp; their families? #CyberSafeChat</p> <p>.....</p> <p>@Panelist1: A10 The FTC's consumer website OnGuardOnline.gov has great resources. #CyberSafeChat</p> <p>.....</p> <p><i>(RT the best responses/call out good responses from participants)</i></p>
<p>3:55 p.m. ET CLOSE</p>	<p>@Moderator: Now it's our guests' turn: Does anyone have an #onlinesafety question they'd like to ask? #CyberSafeTalk</p> <p>.....</p> <p>@Panelist1: Make sure to visit our website _____ for more helpful information! #CyberSafeChat</p> <p>.....</p> <p>@Moderator: That's about all the time we have for today! Do our panelists have anything else to add? #CyberSafeChat</p> <p>.....</p> <p>@Moderator: Thanks for joining us for our _____ Twitter chat! #CyberSafeChat</p>

A

B

C

D

E

F

G

H

I

J

K

L



### Examples of Twitter Chat Scripts

#### Script#2: Online Safety for Small Businesses

Mock information, including the moderator questions and responses from one panelist.

#### Online Safety at Home #CyberSafeChat Twitter Chat [INSERT DATE, TIME, ETC.]

Brand	Organizations	Facebook	Twitter
Theme / Hashtags	General Online Safety Join ____ as we discuss _____. Learn ____, ____ and ____ at this chat. #_____		
Panelists	Moderator: @Moderator Panelists: @Panelist1		

#### Promotional Tweets to Send Out Before and During the Chat

Twitter

Join \_\_, \_\_\_\_, \_\_\_\_ for a #Twitter chat \_\_\_\_ at \_\_. Use #\_\_ to join!

Learn \_\_\_\_\_ at our \_\_\_\_\_ #Twitter chat on \_\_\_\_\_ at \_\_. Use #\_\_\_\_ to join!

Brand on Facebook

Like us on #Facebook for more:

Brand on Twitter

Stay connected after our #Twitter Chat by following \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_ #SmallBizChat

Additional Info

Stay informed and get and get #onlinesafety tips for your small biz here: ((URLS to our websites)) #SmallBizChat

#### Welcome and Intro Tweets

2:50 p.m. ET

Only 10 more minutes until the #smallbiz #onlinesafety Twitter Chat! Use #SmallBizChat to join!

3:00 p.m. ET

@Moderator: Welcome to our #smallbiz #onlinesafety #Twitter chat! #SmallBizChat



3:05 p.m. ET  
QUESTION 1

3:10 p.m. ET  
QUESTION2

@Moderator: Today we'll be talking about ways to keep your small business safe online. #SmallBizChat

@Moderator: Our guests are \_\_\_\_\_ #SmallBizChat

@Moderator: Let's have them introduce themselves! #SmallBiz-Chat

@Panelist1: Hi! We are \_\_\_\_\_ and our mission is \_\_\_\_\_. #Small-BizChat

@Panelist1: We're thrilled to be a part of this #Twitter chat & happy to help empower people with resources to stay safer on-line. #SmallBizChat

*(Allow other panelists to introduce themselves.)*

@Moderator: Great! Who else do we have joining us for our #CyberSafeChat today?

*(Moderator should acknowledge and welcome some people who respond to this tweet.)*

@Moderator: Let's get started! Here comes our first question.... #SmallBizChat

@Moderator: Q1: What's the best thing #smallbiz owners can do to protect the company/employees/customers from #online threats? #SmallBizChat

@Panelist1: A1: Make sure all of the devices have the latest operating systems, software, anti-virus, apps & web browsers. Update regularly!#SmallBizChat

*(Wait about 3 minutes for people to respond and RT the best responses/call out good responses from participants)*

@Moderator: Wow! Those were some great responses!

@Moderator: Here's Q2: what are other ways a #smallbiz can stay safe online? #SmallBizChat

@Panelist1:A2: #Smallbiz should assess their risks, create a #cybersecurity plan & train employees to have good online practices. #SmallBizChat

@Panelist1: A2: Employees are weakest link: educate about Internet safety, train to be wary of email attachments, links from unknown sources. #SmallBizChat

*(RT the best responses/call out good responses from participants)*

3:14 p.m. ET  
QUESTION 3

@Moderator: Q3: Protecting customers & gaining trust is critical for #smallbiz. @Panelist1 how do you accomplish it? #SmallBizChat

@Panelist1: A3: Have a #privacy policy, know what personal info you have, how you store it and who has access to it. #SmallBizChat

@Panelist1: A3: Also, delete data you don't need & keep personal info secure. #SmallBizChat

*(RT the best responses/call out good responses from participants)*

3:18 p.m. ET  
QUESTION 4

@Moderator: Q4: Many times, #smallbiz owners think they are too small to be a target for #cybercriminals. Should they believe this? #SmallBizChat

@Panelist1: A4: It's important for everyone – including #smallbiz – to understand that they could be a target for a #cyber attack. #SmallBizChat

*(RT the best responses/call out good responses from participants)*

3:21 p.m. ET  
QUESTION 5

@Moderator: Q5: If #smallbiz owners do encounter a breach or become a victim of #cybercrime, where should they report the incident? #SmallBizChat

@Panelist1: A5: Report incidents to the U.S. Computer Emergency Readiness Team (@USCERT\_gov) at: <https://forms.us-cert.gov/report/> #SmallBizChat

*(RT the best responses/call out good responses from participants)*

3:25 p.m. ET  
QUESTION 6

@Moderator: As we mentioned before, it's a good idea for #smallbiz to create a #cybersecurity plan. #SmallBiz Chat

@Moderator: Q6: Panelists, can you give us some elements of a #cybersecurity plan? #SmallBizChat

@Panelist1: A6: A comprehensive #cybersecurity plan focuses on 3 key areas: prevention, resolution & restitution. #SmallBizChat

@Panelist1: A6: The @FCC has a #SmallBiz #Cyber Planner that can help: <http://www.fcc.gov/cyberplanner> #SmallBizChat

*(RT the best responses/call out good responses from participants)*

3:29 p.m. ET  
QUESTION 7

@Moderator: Let's go back to talking about employees. #SmallBiz-Chat

@Moderator: Q7: What can #smallbiz owners do to raise #online-safety awareness in their office? #SmallBizChat

3:33 p.m. ET  
QUESTION 8

@Panelist1: A7: Train your employees & teach them good #online-safety habits. #SmallBizChat

@Panelist1: A7: You should also encourage employees to come forward if they notice something wrong. #SmallBizChat

*(RT the best responses/call out good responses from participants)*

@Moderator: BYOD (Bring Your Own #Device) is becoming increasingly popular in the workplace. #SmallBizChat

@Moderator: Q8: What do #smallbiz owners need to know about BYOD? #SmallBizChat

@Panelist1: A8: Regardless of #BYOD, it's a good idea to have a formal written #Internet security policy for employees. #SmallBizChat

@Panelist1: A8: Employees' devices should always have the latest software, OS, web browsers, anti-virus protection, web browsers & apps. #SmallBizChat

*(RT the best responses/call out good responses from participants)*

3:36 p.m. ET  
QUESTION 9

@Moderator: #Phishing & social engineering are common tools #cybercriminals use to

@Moderator: Q9: What are some ways to #phishing & what should #smallbiz owners do to report it? #SmallBizChat

@Panelist1: A9: Typos and misspellings are common signs of #phishing. #SmallBizChat

@Panelist1: A9: Never click on a suspicious URL. Instead, type the URL in your browser or use a search engine to find the website. #SmallBizChat

@Panelist1: A9: You can report #phishing by forwarding the #email to: spam@uce.gov #SmallBizChat

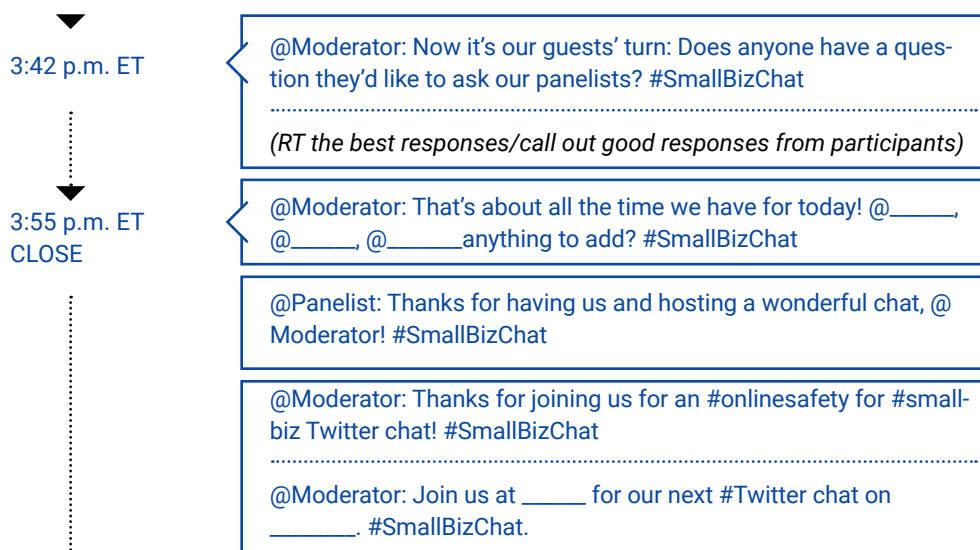
*(RT the best responses/call out good responses from participants)*

3:39 p.m. ET  
QUESTION 10

@Moderator: Q10: What other #onlinesafety resources do you recommend for #smallbiz? #SmallBizChat

@Panelist1: A10: The U.S. Chamber of Commerce (@Commerce-Gov) has this toolkit for #smallbiz: <https://www.uschamber.com/issue-brief/Internet-security-essentials-business-20> #SmallBizChat

*(RT the best responses/call out good responses from participants)*



## Twitter Chat Resources

### Twitter Platforms

You can of course access your Twitter account(s) on Twitter.com, but here is a list of Twitter clients available for download. All of them are free, with added features that are available for a fee:

**Buffer:**

<https://bufferapp.com/>

**Hootsuite:**

<https://hootsuite.com/>

**Janetter:**

<http://janetter.net/>

**Sobees (Windows devices only):**

<http://www.sobees.com/social-media-clients>

**TweetDeck (owned by Twitter):**

<https://about.twitter.com/products/tweetdeck>

**Twitterrific (Apple devices only):**

<http://tweetchup.com/>

### Tools for Creating Virtual Chat Rooms:

Many of these require logging in and/or obtaining access to your Twitter account. Most contain an automatic URL shortener and will automatically add the designated hashtag in your tweets.

**Nurph:**

<http://nurph.com/>

**Tchat.io:**

<http://www.tchat.io/>

**Tweetchat:**

<http://tweetchat.com>

**Twubs:**

<http://twubs.com/>

## Analytics Tools:

Many of these services are free or offer free trials, but have added features that come with a subscription:

**Buffer:**

<https://bufferapp.com/>

**Crowdboost:**

<http://crowdboost.com/>

**Simply Measured:**

<http://simplymeasured.com/>

**Topsy:**

<http://topsy.com/>

**Tweetchip:**

<http://tweetchup.com/>

**Twitter (Must advertise with Twitter or install code within your website):**

<https://analytics.twitter.com/about>

**Twitonomy:**

<http://www.twitonomy.com/>

## URL Shorteners:

These services also provide analytics, so you can see how many people visited a specific URL you promoted during a Twitter chat.

**Bitly:**

<https://bitly.com/>

**Google:**

<https://goo.gl/w>

A

B

C

D

E

F

G

H

I

J

K

L

## J

## Infographics

Infographics are a great way to tell a story using a complex web of data and are so much interesting and visually appealing than traditional graphs. Because of their visual appeal make for excellent social media content that get shared over and over. These infographics are good examples of how to use data to tell the cybersecurity story for different audiences.

## General Public

**Canadian Online/Mobile Surfing Habits and Concerns (McAfee)**

<http://www.computerdealernews.com/news/mcafee-adds-applock-to-mobile-security-offering/11243>

**'Tis the Season to Be Careful: Avoid the 12 Scams of the Holidays (McAfee)**

<http://promos.mcafee.com/offer.aspx?id=565846&cid=131941>

## Youth &amp; Family

**The Cybersecurity Lives of Millennials (National Cybersecurity Alliance)**

<http://staysafeonline.org/stay-safe-online/resources/the-cybersecurity-lives-of-millennials-infographic>

**Parental Control: A Safe and Secure online experience for your kids (Kaspersky)**

<http://usa.kaspersky.com/Internet-security-center/infographics/kids-online>

## Education

**State of U.S. Cyber Education (National Cybersecurity Alliance)**

<http://staysafeonline.org/stay-safe-online/resources/>

## Business

**How Tech Companies Prepare for Cyber Attacks (Silicon Valley Bank)**

<http://www.svb.com/cybersecurity-report-infographic/>

**IT Security (DELL)**

<http://www.infographicsarchive.com/tech-and-gadgets/it-security/#prettyPhoto>

**¿Cuánto Cuestan Mis Datos? (Symantec)**

<http://www.symantec.com/connect/es/blogs/cuanto-cuestan-los-datos-robados-y-servicios-de-ataque-en-el-mercado-clandestino>

**Risky Business: Malware Threats from Unlicensed Software (Business Software Alliance)**

[http://globalstudy.bsa.org/2013/Malware/ig\\_malware\\_en.pdf](http://globalstudy.bsa.org/2013/Malware/ig_malware_en.pdf)

[http://globalstudy.bsa.org/2013/Malware/ig\\_malware\\_es.PDF](http://globalstudy.bsa.org/2013/Malware/ig_malware_es.PDF)

A

B

C

D

E

F

G

H

I

J

K

L

## Resources

### General public

**STOP. THINK. CONNECT.**  
[www.stopthinkconnect.org](http://www.stopthinkconnect.org)

STOP. THINK. CONNECT. offers tips and advice for parents on Internet safety and security, cyberbullying, mobile devices and gaming. In addition to the English language materials, there are limited resources available in Spanish, Portuguese, French, Japanese and Russian.

<http://stopthinkconnect.org/resources/>

**SAFE INTERNET DAY**  
<http://www.saferinternet.org/safer-internet-day>

Safer Internet Day (SID) is organised by Insafe in February of each year to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people across the world.

**Español**  
<http://www.saferinternet.org/resources>

**Français**  
<http://www.saferinternet.org/resources>

**Português**  
<http://www.saferinternet.org/resources>

**MICROSOFT**  
<http://www.microsoft.com/security/default.aspx>

Microsoft is the industry leader in online safety and security consumer education. They have developed a comprehensive suite of materials and resources that include information for parents

and children on Internet safety, Internet security and digital privacy. Resources include online and downloadable content, PowerPoints, eBooks (for teens) and videos. Materials are available in numerous languages including:

**Español**  
<http://www.microsoft.com/es-xl/security/default.aspx>

**Français**  
<http://www.microsoft.com/fr-fr/security/default.aspx>

**Português**  
<http://www.microsoft.com/pt-pt/security/default.aspx>

**FACEBOOK**  
<http://www.facebook.com/safety>

Facebook is committed to online safety for young people. A variety of tools and resources are available to help parents navigate account and privacy settings, help parents understand social media and how to help their teens navigate the pitfalls of social media and managing a digital life.

**NORTON BY SYMANTEC**  
<http://us.norton.com/family-resources/>

Norton's family resource center has tips for parents, teens and children. Norton also has a downloadable Family Online Safety Guide available in several languages.

**English**  
<http://us.norton.com/online-safety-guide>

## Español

[http://now.symassets.com/now/en/pu/images/Promotions/onlineSafetyGuide/BR-00386-SL-FamilyOnlineSafetyGuide\\_3rdEd.pdf](http://now.symassets.com/now/en/pu/images/Promotions/onlineSafetyGuide/BR-00386-SL-FamilyOnlineSafetyGuide_3rdEd.pdf)

## Français

[http://www.symantec.com/content/en/us/home\\_homeoffice/media/theme/parentresources/FOSG-French.pdf](http://www.symantec.com/content/en/us/home_homeoffice/media/theme/parentresources/FOSG-French.pdf)

## MCAFFEE

<http://www.thinkbeforeyoulinkinschool.com/family>

## GOOGLE

<https://www.google.com/safetycenter/>

Google's safety center has tools and resources for families that cover online safety and security. In addition to basic online safety and security guidance, the resource center has information on how to set up family friendly search filters, use app ratings, and how to control access to approved games and apps.

## Youth, Parent and Educators

The following resources have great materials for parents and youth. Except where noted, all of the resources are available for free (all corporate resources included in this list are free). These resources are all in English, some are available in other languages including Spanish, French, and Portuguese.

## INTERNET WATCH FOUNDATION

[www.iwf.org.uk](http://www.iwf.org.uk)

The Internet Watch Foundation (IWF) deals specifically with child abuse and criminally obscene images hosted in the UK and internationally. IWF works in partnership with the online industry, law enforcement, government, and international partners. It is a charity and self-regulatory body with over 100 members from the online industry.

## Español

[www.iwf.org.uk](http://www.iwf.org.uk)

## CHILDNET INTERNATIONAL

[www.childnet.com](http://www.childnet.com)

Childnet International is a non-profit organization working in partnership with others around the world to help make the internet a great and safe place for children. The website hosts a number of recommended resources for young people, parents, carers and teachers.

## PROTECIONONLINE.COM

<http://www.protecciononline.com>

Protecciononline.com is an organization with a wealth of knowledge and resources for safety online. The organization was created for the purposes of making available the best recommendations on the use of new technologies in a safe manner. This is done through the promotion of good habits online, cyber citizenship and actions that mitigate online threats.

## FAMILY ONLINE SAFETY INSTITUTE (FOSI)

[www.fosi.org](http://www.fosi.org)

FOSI is an NGO, based in the United States and the United Kingdom, which focuses on online safety for children and families. They have a wealth of resources for parents to learn about online safety, privacy and parenting digital kids. In addition to developing education resources, FOSI also develops policy briefings and conducts research.

## IKEEPSAFE

iKeepSafe is a United States based NGO focused on online safety and security, digital citizenship and privacy for children. Free resources available for parents include.

## Faux Paw, a series of digital books for young children

<http://www.ikeepSAFE.org/parents/faux-paw/>



**BEAPRO Apps for Facebook and Android**

This app helps parents assess the digital behavior in their household, offers experts tips and resources, and advice on how to pass information along to children.

<http://www.ikeepsafe.org/beapro-parent-app/>

**Social media guidance**

<http://ikeepcurrent.org/>

**Videos**

<http://www.ikeepsafe.org/videos/>

**COMMON SENSE MEDIA**

[www.commonsensemedia.org](http://www.commonsensemedia.org)

Common Sense Media is a U.S. based NGO whose mission to “empower parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids’ lives.”

Common Sense media provides guidance for parents on a variety of digital topics including a list of great, age appropriate apps, cyberbullying, screen time, privacy and Internet safety, and social media.

**Common Sense Media family resources:**

<https://www.commonsensemedia.org/educators/family-tip-sheets>

**En Español**

<https://www.commonsensemedia.org/educators/family-tip-sheets>

**STAYSAFEONLINE.ORG**

[www.staysafeonline.org](http://www.staysafeonline.org)

Staysafeonline.org is a website run by the National Cybersecurity Alliance (NCSA) a U.S based NGO whose

mission is “to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets.”

Staysafeonline.org has a wealth of resources for parents including information on digital citizenship, cyberbullying, parental control and online gaming. Parents will also find resources on basic cybersecurity best practices, identity theft, mobile devices and social networking.

**NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC) NETSMARTZ WORKSHOP**

<http://www.netsmartz.org/>

NetSmartz Workshop, a program of the National Center for Missing & Exploited Children offers resources and materials for parents, teens, tweens and children. Videos, games, quizzes and online tips cover a range of issues from identity theft, cyberbullying, mobile devices, social media, cybersecurity and gaming.

**FTC ONGUARDONLINE**

[www.onguardonline.gov/](http://www.onguardonline.gov/)

**Español**

[www.alertaenlinea.gov/](http://www.alertaenlinea.gov/)

OnguardOnline.gov is a consumer online safety and security website of the United States Federal Trade Commission. There is a wealth of information and resources for parents, teens and children about cybersecurity, online safety and privacy. Resources include tips, games, and videos. Onguardonline has also put together a great downloadable book to help parents discuss online safety issues with their children.

(<http://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf>)

A

B

C

D

E

F

G

H

I

J

K

L

A

B

C

D

E

F

G

H

I

J

K

L

## Business

### STOP. THINK. CONNECT.

STOP. THINK. CONNECT. offers tips and advice businesses can use to begin making their businesses more secure as well as materials that can downloaded be posted in the workplace to educate employees. In addition to the English language materials, there are limited resources available in Spanish, Portuguese, French, Japanese and Russian.

<http://stopthinkconnect.org/resources/>

### UNITED STATES FEDERAL COMMUNICATIONS COMMISSION (FCC)

The FCC has developed a cybersecurity planning tool for small businesses. The planner helps evaluate your cybersecurity readiness and create a plan focused on prevention, resolution and restitution. In addition to the planner they have list of additional resources.

<http://www.fcc.gov/cyberforsmallbiz>

### UNITED STATES DEPARTMENT OF HOMELAND SECURITY COMPUTER EMERGENCY READINESS TEAM (US-CERT)

US-CERT is a great resource for detailed information on all kinds of cybersecurity threats, technical information and guidance on how to protect your networks and devices. They also have an RSS feed you can subscribe to for up-to-date information on cybersecurity issues.

<https://www.us-cert.gov/ncas/tips>

### FEDERAL TRADE COMMISSION (FTC)

While the FTC's website isn't specifically aimed at business, much of information is valuable for small business.

<http://www.onguardonline.gov/topics/secure-your-computer>

### Español

<http://www.alertaenlinea.gov/temas/proteja-su-computadora>

### CENTER FOR INTERNET SECURITY (CIS)

<https://www.cisecurity.org/>

CIS has resources businesses can use to learn some cybersecurity basics (securing login credentials, social media accounts, online banking safety). CIS is connected with the Multi-State Information Sharing and Analysis Center (MSISAC) that has daily tips, a newsletter and links to free training resources.

<http://msisac.cisecurity.org/>

### NATIONAL CYBERSECURITY ALLIANCE (NCSA)

NCSA has good resources for small businesses looking to educate themselves about how to stay safe online.

<http://staysafeonline.org/business-safe-online/>

### MICROSOFT

Microsoft has great information for the workplace.

<http://www.microsoft.com/security/default.aspx>

### Español

<http://www.microsoft.com/es-xl/security/default.aspx>

### Français

<http://www.microsoft.com/fr-fr/security/default.aspx>

### Português

<http://www.microsoft.com/pt-pt/security/default.aspx>

## Examples of Research & Surveys

### NATIONAL CYBERSECURITY ALLIANCE (NCSA)

NCSA has conducted a number of small business surveys on a variety of topics over the past several years.

<http://staysafeonline.org/business-safe-online/resources/>

### PWC

Global State of Information Security Survey 2015

<http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml>

### EY

Global Information Security Survey 2014

[http://www.ey.com/Publication/vwLUAs-sets/EY-global-information-security-survey-2014/\\$FILE/EY-global-information-security-survey-2014.pdf](http://www.ey.com/Publication/vwLUAs-sets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf)

Microsoft has commissioned numerous research studies looking at issues such as mobile use, cybersecurity education, online bullying, online gaming and online reputation management.

### PEW RESEARCH INTERNET PROJECT

<http://www.pewInternet.org/2013/05/21/teens-social-media-and-privacy/>

Teens, Social Media, and Privacy

### RISKY BUSINESS: MALWARE THREATS FROM UNLICENSED SOFTWARE (BUSINESS SOFTWARE ALLIANCE)

<http://globalstudy.bsa.org/2013/index.html>

### Español

[http://globalstudy.bsa.org/2013/Malware/study\\_malware\\_esmx.pdf](http://globalstudy.bsa.org/2013/Malware/study_malware_esmx.pdf)

A

B

C

D

E

F

G

H

I

J

K

L

## Parenting/Family

### FOSI: PARENTING IN THE DIGITAL AGE 2014

<https://www.fosi.org/policy-research/parenting-digital-age/>

### IKEEPPSAFE: PARENT SAFETY INDEX REPORT 2013

[http://storage.googleapis.com/ikeepsafe/BEaPRO%20Parent/BEaPRO\\_Parent\\_Index\\_Report.pdf](http://storage.googleapis.com/ikeepsafe/BEaPRO%20Parent/BEaPRO_Parent_Index_Report.pdf)

### MICROSOFT

<http://www.microsoft.com/security/resources/research-studies.aspx>



## Sample messages from STOP. THINK. CONNECT

A

B

C

D

E

F

G

H

I

J

K

L

STOP. THINK. CONNECT.™ is the global cybersecurity awareness campaign to help all digital citizens stay safer and more secure online.

STOP. THINK. CONNECT. was developed by a coalition of private companies, non-profits and government organizations under the guidance of the Anti-Phishing Working Group (APWG) and National Cybersecurity Alliance (NCSA). Extensive research was conducted to inform the campaign of messages that would not only raise awareness about cybersecurity but also inspire people to change their behavior. In October of 2010 the campaign was launched by the STOP. THINK. CONNECT. Messaging Convention in partnership with the U.S. government, including the White House. The campaign is overseen by the APWG and NCSA. Since the initial launch in the U.S. the campaign has gained global traction. Canada, Japan, Malaysia, Panama, Paraguay and Uruguay have all signed on to the campaign. The Organization of American States has signed an MOU to adopt and support the campaign.

### Goals and Objectives of STOP. THINK. CONNECT.

"We will encourage all Internet users to be more vigilant about practicing safe, online habits; ensure that Internet safety is perceived as a shared responsibility at home, in the workplace, and throughout our communities; and transform the way the public and private sectors and the U.S. federal government collaborate to make cybersecurity a reality.

Our goal is to help people understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior."

### We aim to:

- Increase and reinforce awareness of cybersecurity, including associated risks and threats, and provide solutions for increasing cybersecurity.
- Communicate approaches and strategies for the public to keep themselves, their families and their communities safer online.
- Shift perception of cybersecurity among the American public from avoidance of the unknown to acknowledgement of shared responsibility.
- Engage the public, the private sector, and state and local governments in our nation's effort to improve cybersecurity.
- Increase the number of national stakeholders and community-based organizations engaged in educating the public about cybersecurity and what people can do to protect themselves online.

The STOP. THINK. CONNECT. campaign is open for anyone to join, there is no cost. All of the materials found at [www.stopthinkconnect.org](http://www.stopthinkconnect.org) are available for anyone to use. Businesses, NGO's and individuals wishing to use the logo on their websites, to create unique materials or modify the already created campaign materials are required to sign a license. There is no cost for the license, it is simply an agreement that the campaign guidelines will be followed and used in manner in which it was intended. To review the license and the accompanying editorial style guidelines see Appendix A & B. Governments that would like to join the campaign are asked to sign a Memorandum of Understanding (MOU). The MOU is an agreement with the STOP. THINK. CONNECT. Messaging Convention stating the intention of the campaign and the government. For more information about international campaign partnerships contact Peter Cassidy at [Peter@apwg.org](mailto:Peter@apwg.org).

## STOP. THINK. CONNECT. Messages

These are the messages associated with the STOP. THINK. CONNECT. campaign. They were developed based on the research used to inform the campaign. All of these messages were carefully crafted to be positive and action oriented. Each primary message is followed by a series of sub-messages that are intended to be positive and action oriented. All of the primary messages can be used with any audience while the sub-messages may appropriate for a more targeted audience. All of these primary messages are the beginning points of a campaign – the messages can be edited or added to as needed for a particular audience.

### Keep a Clean Machine.

- *Keep security software current:*  
Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- *Automate software updates:*  
Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- *Protect all devices that connect to the Internet:*  
Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- *Plug & scan:*  
USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

### Protect Your Personal Information.

- *Secure your accounts:*  
Ask for protection beyond passwords. Many account providers now offer additional ways for you to verify who you are before you conduct business on that site.

- *Make passwords long and strong:*  
Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- *Unique account, unique password:*  
Separate passwords for every account helps to thwart cybercriminals.
- *Write it down and keep it safe:*  
Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- *Own your online presence:*  
Set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

### Connect with Care.

- *When in doubt, throw it out:*  
Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- *Get savvy about WiFi hotspots:*  
Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- *Protect your \$\$:*  
When banking and shopping, check to be sure the sites are security enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "Http://" is not secure.

### Be Web Wise.

- *Stay current:*  
Keep pace with new ways to stay safe online. Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.



A

B

C

D

E

F

G

H

I

J

K

L

- *Think before you act:*

Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.

- *Back it up:*

Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

### **Be a Good Online Citizen.**

- *Safer for me more secure for all:*

What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

- *Post only about others as you have them post about you.*

- *Help the authorities fight cybercrime:*

Report stolen finances, identities and cybercrime to [insert local reporting agency information].











Organization of  
American States | More rights  
for more people

17th Street and Constitution Ave., NW  
Washington, D.C., 20006-4499  
United States of America

**[www.oas.org](http://www.oas.org)**