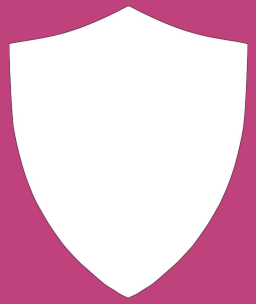
Module 1:



Security & Data Protection

Objectives:

At the end of this module you will be able to:

- ➔ *Evaluate the strength of a password and demonstrate an understanding of optimal, safe password usage.*
- ➔ *Identify the possible risks, vulnerabilities, and indicators of malware infection.*
- ➔ *Demonstrate the ability to protect against social engineering and identify malicious communication*
- ➔ *Define necessary protection measures and determine the precautions needed in public spaces.*

DQ Pro

Module 1: Security & Data Protection

Section 1: Password Basics

Letting you in while keeping the bad guys out - Securing Our Company's Data

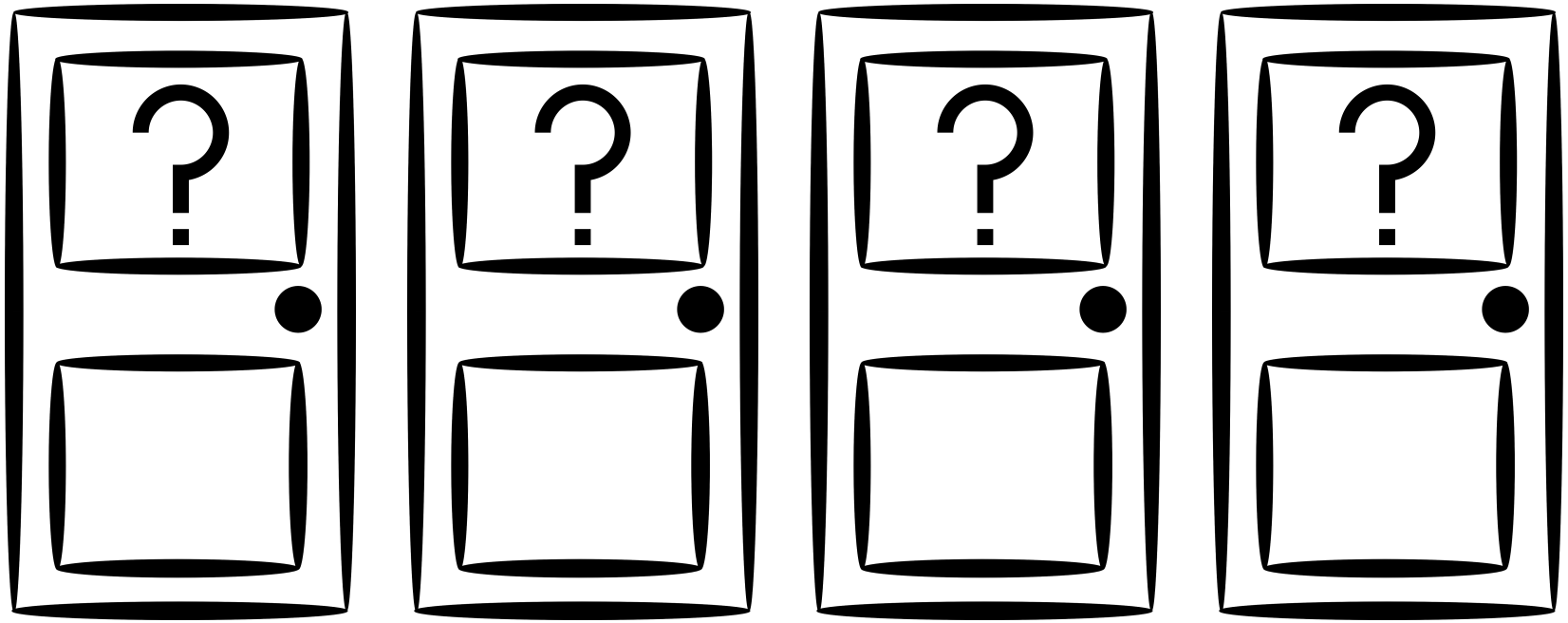
Essential Questions:

1. What makes a password strong or weak?
2. What are the risks if your password is weak or easy-to-breach?
3. Should you change your password regularly?
4. Are there tips to help you remember your many passwords?

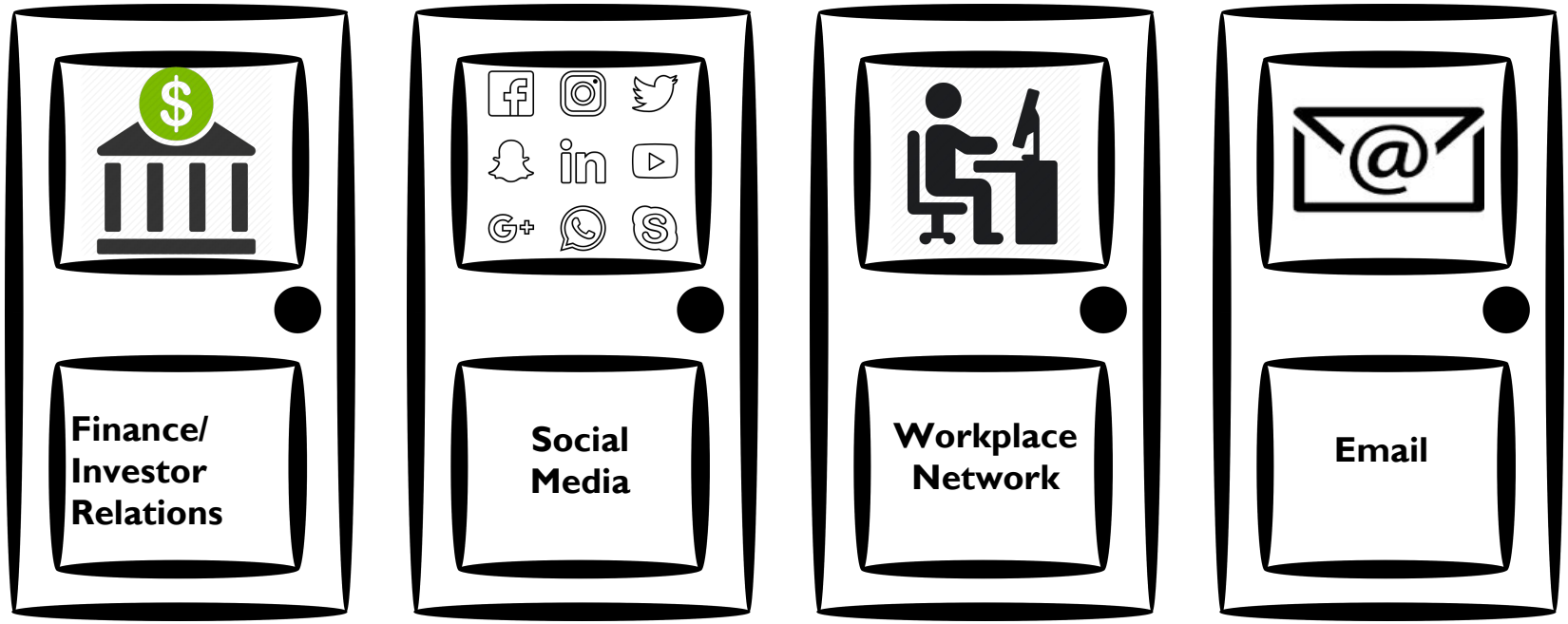
Did you know? A weak password could lead to loss of money, intellectual property, company reputation, brand value, and your identity.

Imagine your password as a key. A password is a unique identifier that you use to keep your devices and data safe. Often, people create a unique and distinctive password, but use it over and over for each device they own or website they join. Or, they create many different passwords, but they are simplistic and contain easily identifiable information, such as anniversary or birth dates. Our company has a set of protocols that you need to use while setting passwords. We will provide you with those at the end of this course.

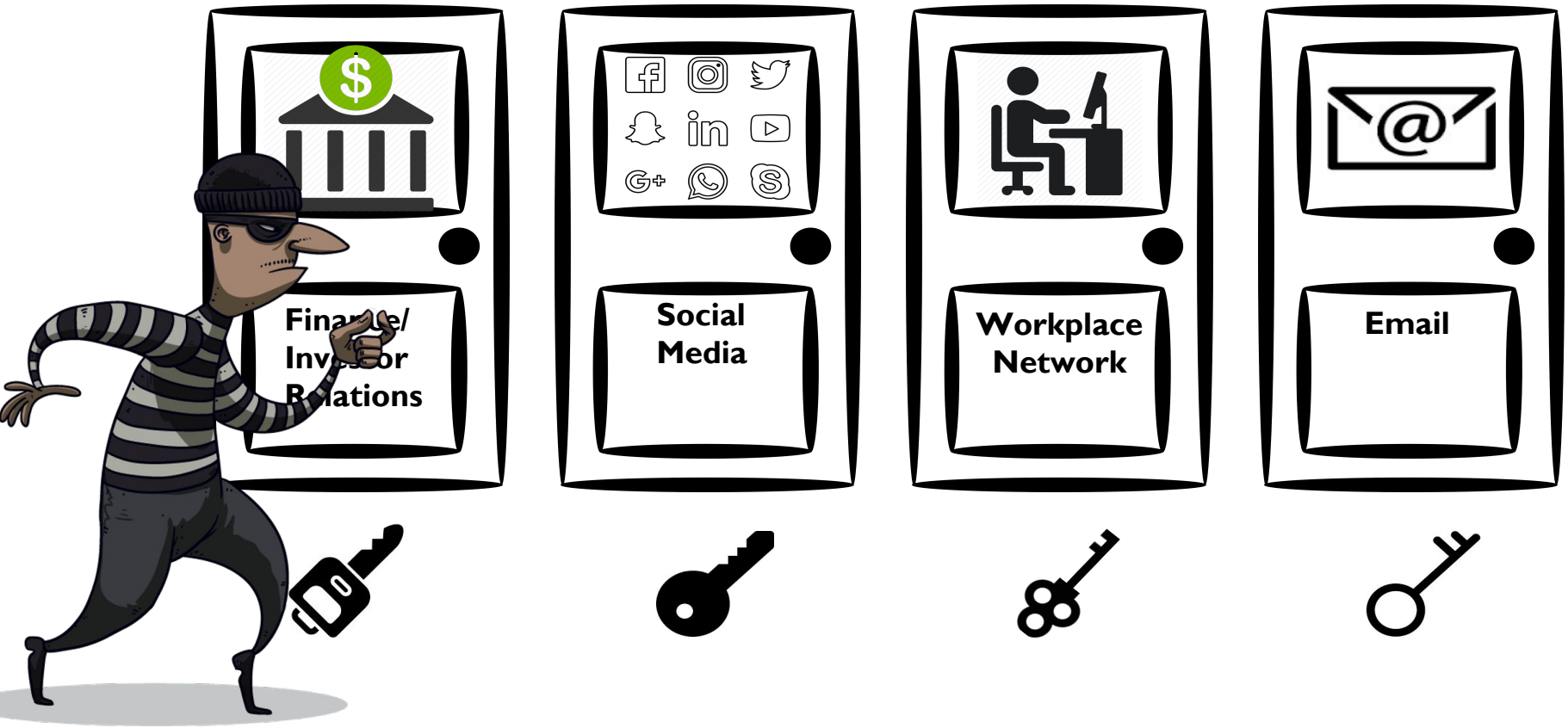
What doors can this key open?



Here are a few examples...



What can happen if these doors are opened by someone other than you?

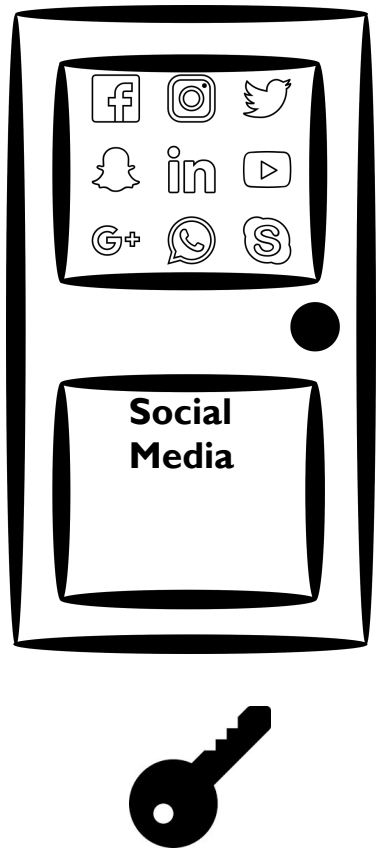


What can happen if these doors are opened by someone other than you?

There can be serious consequences if someone is able to hack your password and gain access to the financial files of the company you work for. Competitors can use information, such as profit and loss records, to their advantage with devastating consequences for your company. Leaked financial information could make negotiations on pricing and deals more difficult. Investor relations may be affected, and SEC (Securities and Exchange Commission) issues on company stock could arise. The leaking of sensitive information could negatively affect the company's reputation.

Source: Javelin Strategy and Research

What can happen if these doors are opened by someone other than you?



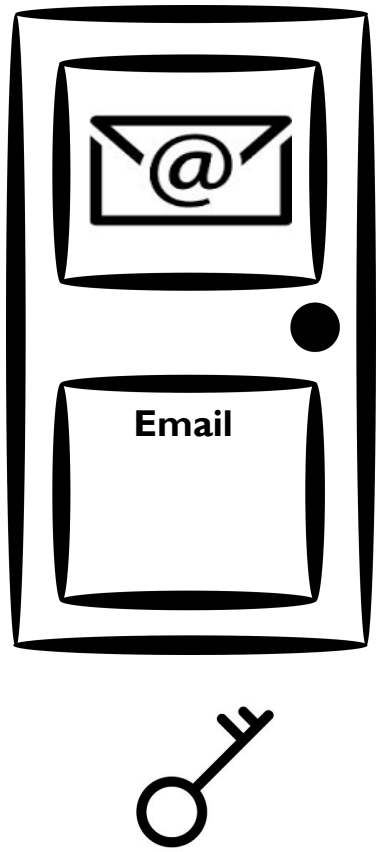
Social media websites, such as Facebook and Twitter, allow you to communicate and share information, but they can also be used to against you. If your password to such sites is hacked, an attacker can post information as if they were you that can have negative consequences for the company you work for. They could harbor grudges against you or the company and spread information that could hurt both. Companies have lost stock valuation because of rumors, false late product shipment dates, production issues, and false financial information. We just need to be careful not to allow anyone to post on your social sites.

What can happen if these doors are opened by someone other than you?

If an attacker is able to gain access to your company's network, they may be able to gain access to sensitive information and files. Company secrets can be exposed, customer accounts may be accessed, employee information, financial records and business plans may be stolen. The consequences for your company could be disastrous!

What can happen if these doors are opened by someone other than you?

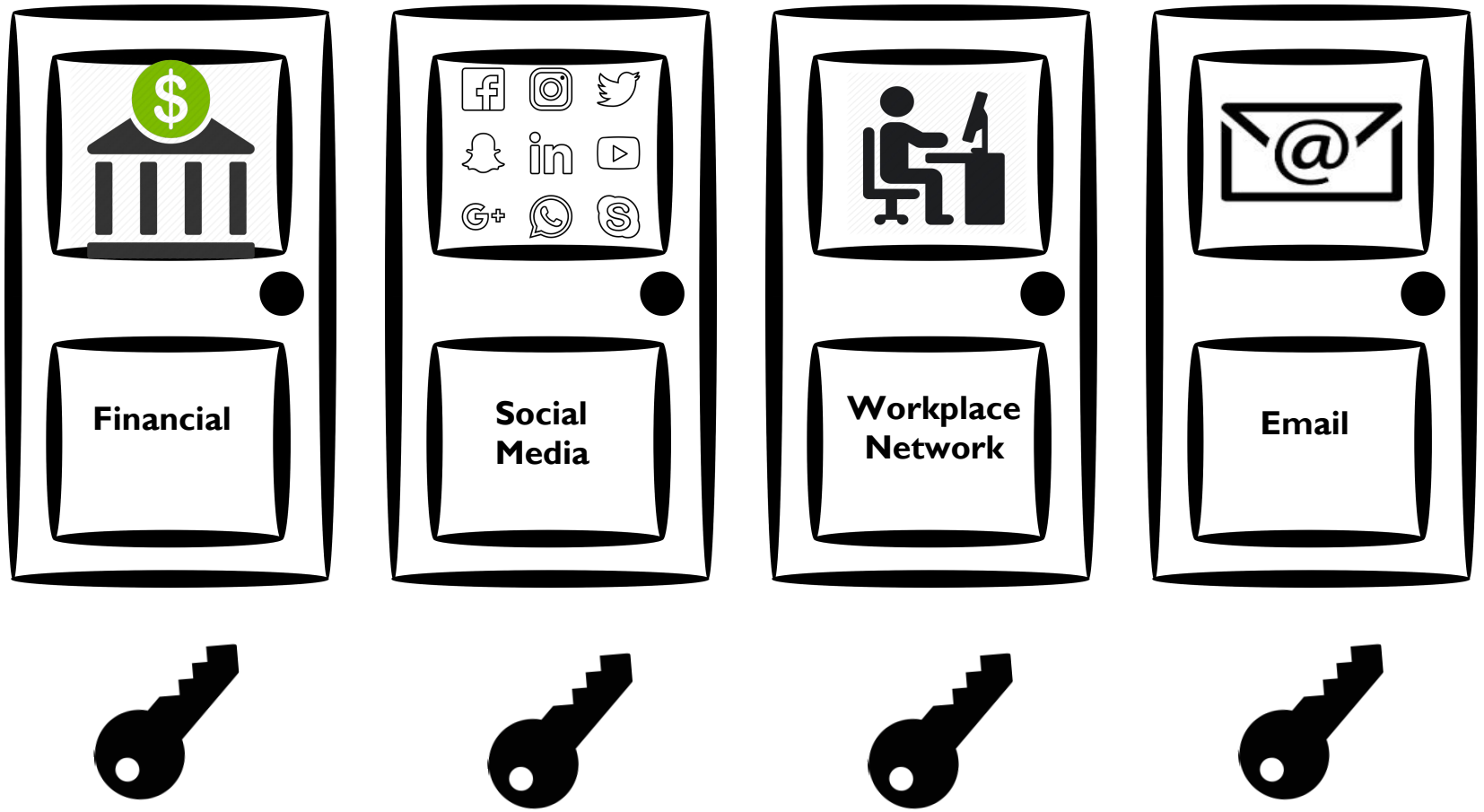
Once someone has access to your email, they can search your inbox for password or screen name reminders, tax documents and other sensitive information, including company information. They can also infect others by sending out scam emails to your work or social networks. One particular scam, the Business Email Compromise Scam (BEC) costs companies 3.1 billion dollars annually (FBI)!



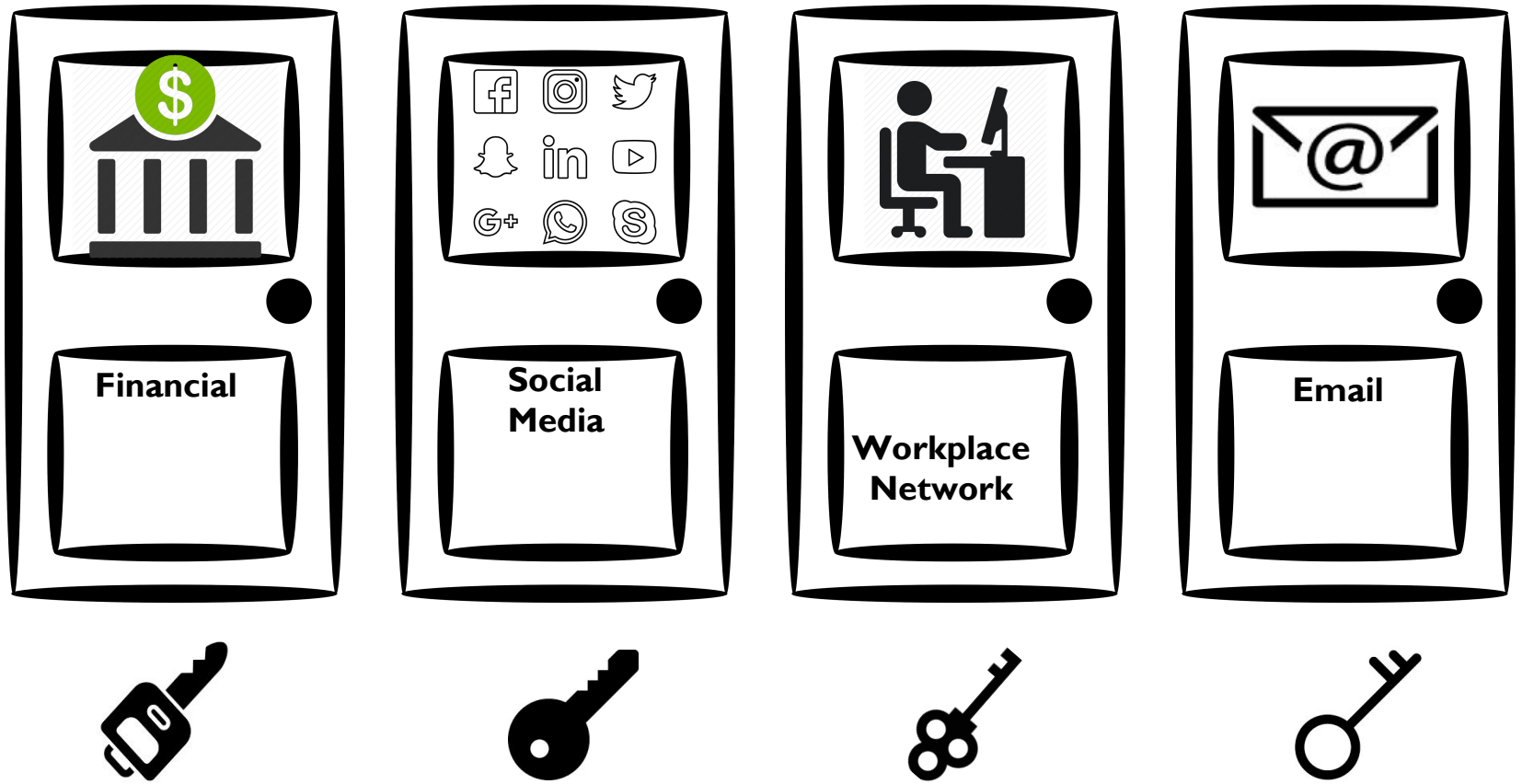
*For more information on BEC scams : FBI

https://www.ic3.gov/media/2016/160614.aspx

If you are using one password, a thief could open up all of these doors!



Creating different passwords for different accounts and application helps you lower the risks.



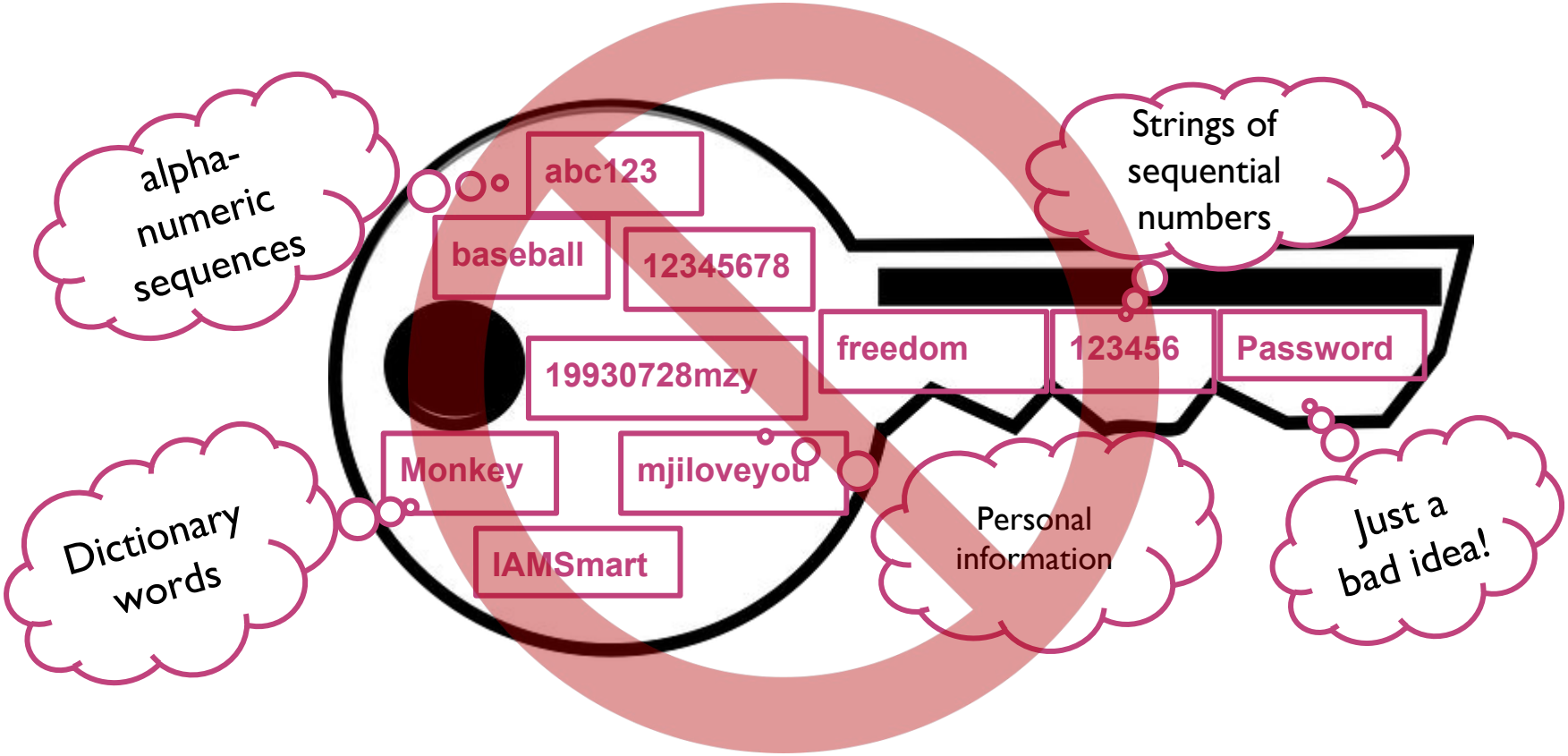
What makes a password weak? What makes a password strong?

The following don'ts are ways that make you password weak and more susceptible to hacking. Read through these to learn what NOT to do.

DON'T USE...

- dictionary words
- personal information, such as: part of your name, birthdate, social security number, or similar information about loved ones.
- sequences or repetitions of numbers and letters.

What makes a password weak?



What makes a password weak? What makes a password strong?

The following dos are ways that make you password strong and less susceptible to hacking. Read through these to learn what to do.

DO USE...

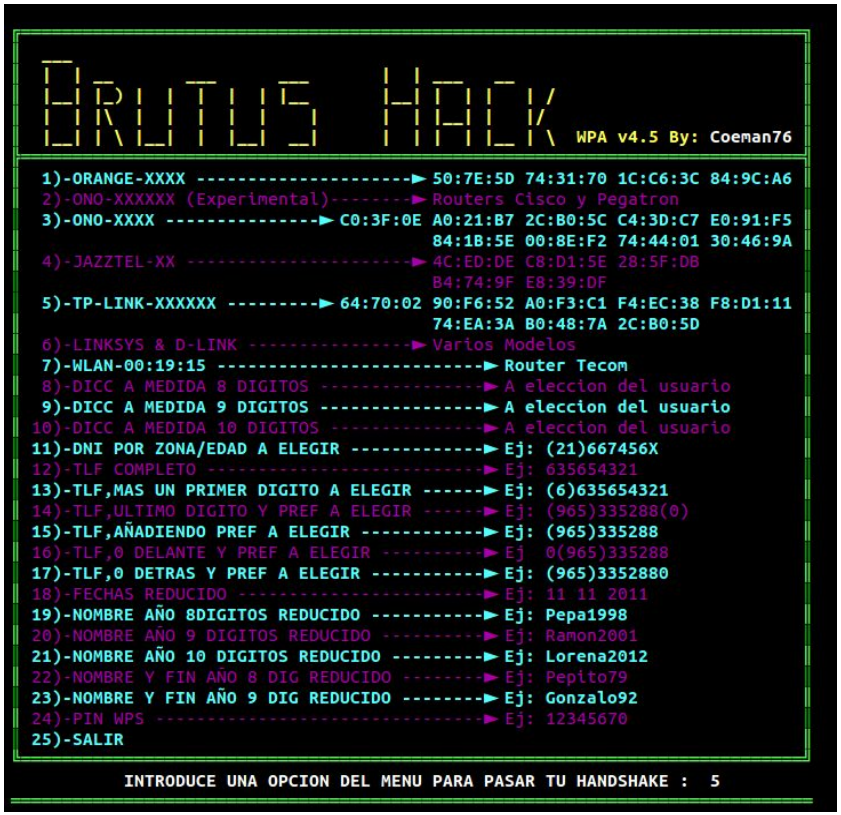
- special characters, such as $, #, &.
- a mixture of upper and lower case letters as well as numbers.
- longer passwords.
- consider using the first letter of each word in a sentence, phrase, song or poem title, adding in numbers and/or special characters.
- an online password strength checker, such as: www.microsoft.com/protect/yourself/password/checker.mspx

Use special characters, such as $, #, &
a mixture of upper and lower case letters as well as numbers.

For example **R@3ct1We$!**

***O#e/L7^iS)**

Use Longer passwords



What is a brute force hack?

A brute force hack is when a hacker runs a program that tries to guess every possible combination of numbers, letters, and characters.

Imagine if your password was 4 characters long, and you could only use the uppercase letters A, B, C, and D. There would only be 35 possibilities!

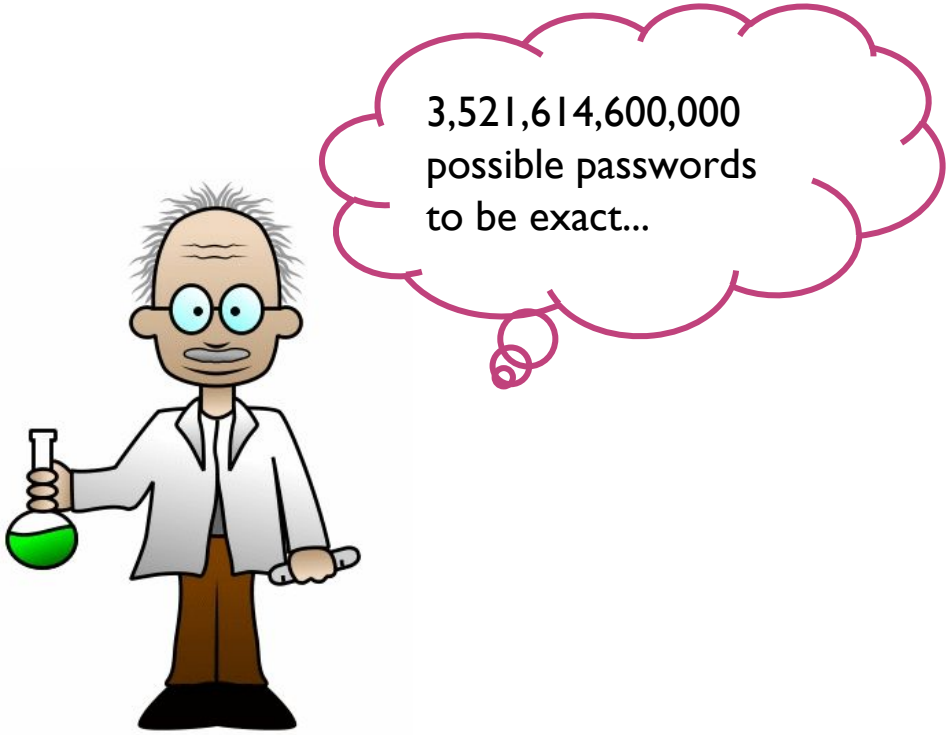
{a,b,c,d} {a,b,d,c} {a,c,b,d} {a,c,d,b} {a,d,b,c} {a,d,c,b}
{b,a,c,d} {b,a,d,c} {b,c,a,d} {b,c,d,a} {b,d,a,c} {b,d,c,a}
{c,a,b,d} {c,a,d,b} {c,b,a,d} {c,b,d,a} {c,d,a,b} {c,d,b,a}
{d,a,b,c} {d,a,c,b} {d,b,a,c} {d,b,c,a} {d,c,a,b} {d,c,b,a}

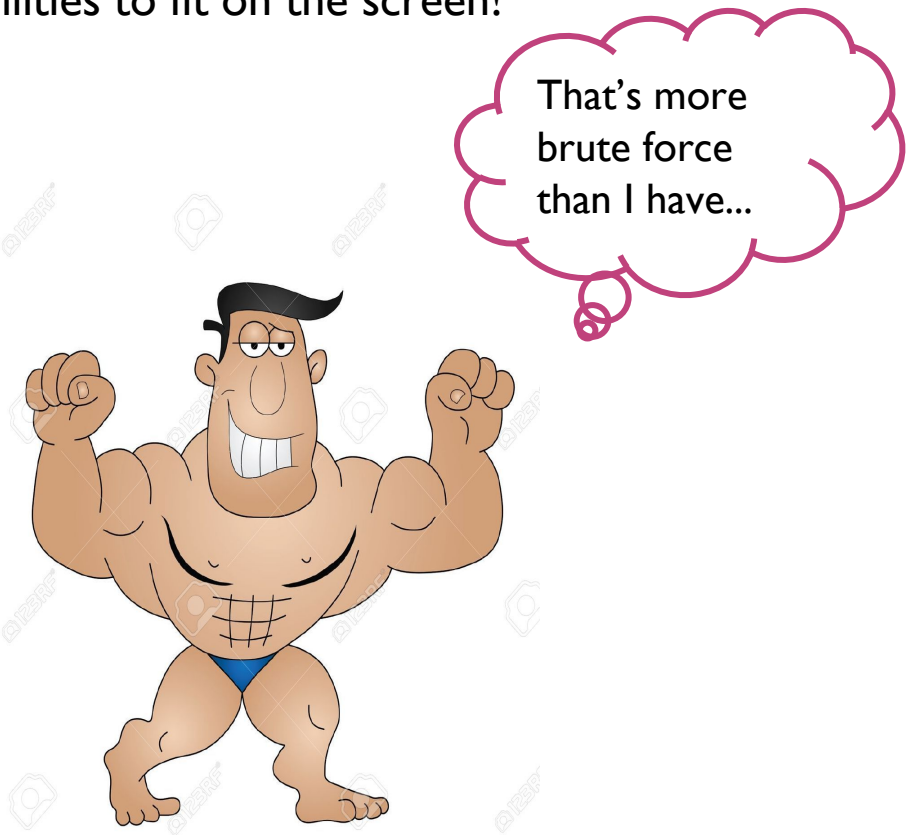
Now imagine it was 7 characters using only A, B,C, and D...the number of possible outcomes is now 120!

{a,a,a,a,a,a,a} {a,a,a,a,a,a,b} {a,a,a,a,a,a,c} {a,a,a,a,a,a,d} {a,a,a,a,a,b,b} {a,a,a,a,a,b,c}
{a,a,a,a,a,b,d} {a,a,a,a,a,c,c} {a,a,a,a,a,c,d} {a,a,a,a,a,d,d} {a,a,a,a,b,b,b} {a,a,a,a,b,b,c}
{a,a,a,a,b,b,d} {a,a,a,a,b,c,c} {a,a,a,a,b,c,d} {a,a,a,a,b,d,d} {a,a,a,a,c,c,c} {a,a,a,a,c,c,d}
{a,a,a,a,c,d,d} {a,a,a,a,d,d,d} {a,a,a,b,b,b,b} {a,a,a,b,b,b,c} {a,a,a,b,b,b,d} {a,a,a,b,b,c,c}
{a,a,a,b,b,c,d} {a,a,a,b,b,d,d} {a,a,a,b,c,c,c} {a,a,a,b,c,c,d} {a,a,a,b,c,d,d} {a,a,a,b,d,d,d}
{a,a,a,c,c,c,c} {a,a,a,c,c,c,d} {a,a,a,c,c,d,d} {a,a,a,c,d,d,d} {a,a,a,d,d,d,d} {a,a,b,b,b,b,b}
{a,a,b,b,b,b,c} {a,a,b,b,b,b,d} {a,a,b,b,b,c,c} {a,a,b,b,b,c,d} {a,a,b,b,b,d,d} {a,a,b,b,c,c,c}
{a,a,b,b,c,c,d} {a,a,b,b,c,d,d} {a,a,b,b,d,d,d} {a,a,b,c,c,c,c} {a,a,b,c,c,c,d} {a,a,b,c,c,d,d}
{a,a,b,c,d,d,d} {a,a,b,d,d,d,d} {a,a,c,c,c,c,c} {a,a,c,c,c,c,d} {a,a,c,c,c,d,d} {a,a,c,c,d,d,d}
{a,a,c,d,d,d,d} {a,a,d,d,d,d,d} {a,b,b,b,b,b,b} {a,b,b,b,b,b,c} {a,b,b,b,b,b,d} {a,b,b,b,b,c,c}
{a,b,b,b,b,c,d} {a,b,b,b,b,d,d} {a,b,b,b,c,c,c} {a,b,b,b,c,c,d} {a,b,b,b,c,d,d} {a,b,b,b,d,d,d}
{a,b,b,c,c,c,c} {a,b,b,c,c,c,d} {a,b,b,c,c,d,d} {a,b,b,c,d,d,d} {a,b,b,d,d,d,d} {a,b,c,c,c,c,c}
{a,b,c,c,c,c,d} {a,b,c,c,c,d,d} {a,b,c,c,d,d,d} {a,b,c,d,d,d,d} {a,b,d,d,d,d,d} {a,c,c,c,c,c,c}
{a,c,c,c,c,c,d} {a,c,c,c,c,d,d} {a,c,c,c,d,d,d} {a,c,c,d,d,d,d} {a,c,d,d,d,d,d} {a,d,d,d,d,d,d}
{b,b,b,b,b,b,b} {b,b,b,b,b,b,c} {b,b,b,b,b,b,d} {b,b,b,b,b,c,c} {b,b,b,b,b,c,d} {b,b,b,b,b,d,d}
{b,b,b,b,c,c,c} {b,b,b,b,c,c,d} {b,b,b,b,c,d,d} {b,b,b,b,d,d,d} {b,b,b,c,c,c,c} {b,b,b,c,c,c,d}
{b,b,b,c,c,d,d} {b,b,b,c,d,d,d} {b,b,b,d,d,d,d} {b,b,c,c,c,c,c} {b,b,c,c,c,c,d} {b,b,c,c,c,d,d}
{b,b,c,c,d,d,d} {b,b,c,d,d,d,d} {b,b,d,d,d,d,d} {b,c,c,c,c,c,c} {b,c,c,c,c,c,d} {b,c,c,c,c,d,d}
{b,c,c,c,d,d,d} {b,c,c,d,d,d,d} {b,c,d,d,d,d,d} {b,d,d,d,d,d,d} {c,c,c,c,c,c,c} {c,c,c,c,c,c,d}
{c,c,c,c,c,d,d} {c,c,c,c,d,d,d} {c,c,c,d,d,d,d} {c,c,d,d,d,d,d} {c,d,d,d,d,d,d} {d,d,d,d,d,d,d}

So how do I protect myself?

What if each of the seven characters was either an upper or lower case letter or a number? Now you have way too many possibilities to fit on the screen!





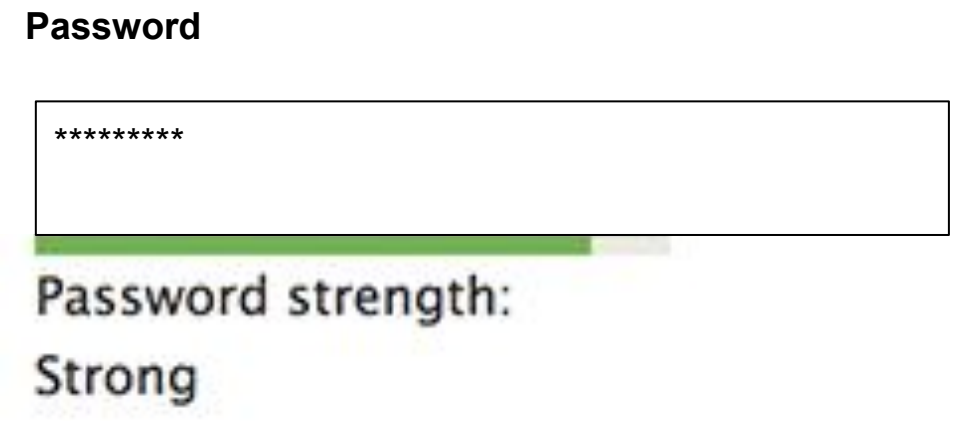
Consider the first letter of each word in a sentence, phrase, song or poem title, adding in number and special characters.

For example

As You Like It, by Shakespeare → 6@YLi*S3!

One apple a day keeps the doctor away → 1A@Dk0TdA^

Based on the dos and don'ts, please create a strong password!



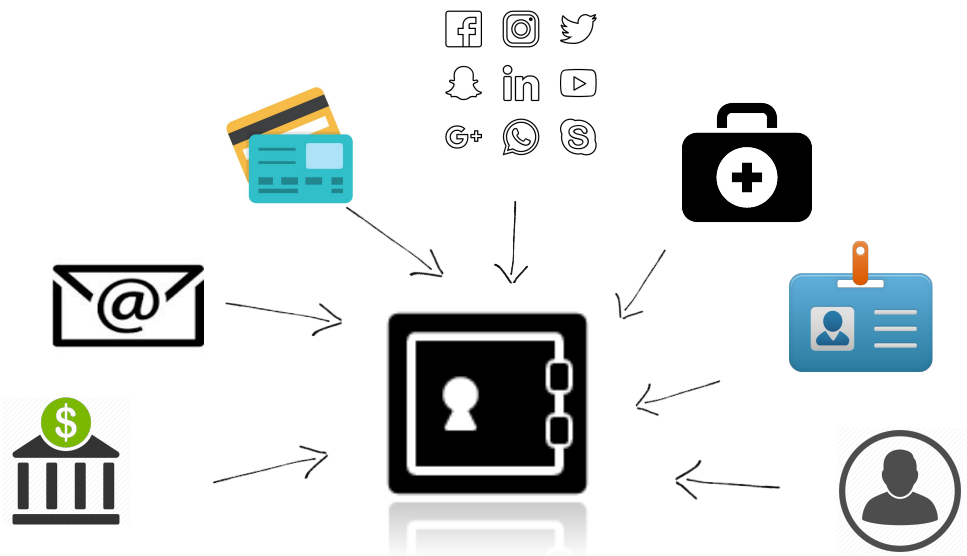
How should I remember my passwords?

Despite admonitions to the contrary, one easy way to remember your passwords is to write them down and keep them in a securely locked place. Never leave them on a Post-It note on your monitor, in an address book, in a desk drawer, or under your keyboard or mouse pad (or any other obvious place).

Imagine you could take all of your keys, or passwords, and lock them up in a safe so that you would only need one key, or password. Well, YOU CAN!

It's called a password manager.

What does a password manager do, you ask?
It makes it easy to securely create, save, and enter strong passwords everywhere. And all you have to remember is ONE password, the one for the password manager. Check with your IT department for a recommendation.



What is a password manager and how does it help?

Password managers store your login information and generate strong passwords for you. They are also useful because with a password manager, the only password you have to remember is the one to open your manager.

Check with your IT Department for recommendations.

How often should I change my password?

Not as often as you might think.

Changing passwords regularly is not as secure as was previously thought. In addition, people who change their passwords often tend to use weaker passwords each time. If you already have a strong password and there is no evidence that your account has been hacked, you probably don't need to change it.

Sometimes, however, there are good reasons to change your password. So if you

- have reason to believe your password has been stolen,
- shared your password with a friend,
- saw someone looking over your shoulder as you were typing your password,
- think you might have just given your password to a phishing website,
- are using a weak password

CHANGE YOUR PASSWORD!

Why is this password weak for Michelle R.(Age 29)?

fr71987twofour

Pick all that apply.

A. Not enough variation of letters and numbers

B. No mix of capital and lowercase letters

C. Some information available via public domain or other sources

D. Contains some element of her name.

DQ Pro

Why is this password strong for Michelle R.(Age 29)?

MR,1994twofour

Pick all that apply.

A. Contains a mixture of letters, numbers, and special characters

B. Does not contain elements of name

C. More than 7 characters

D. Does not contain dates that can be deduced from information available via public domain.

DQ Pro

Which of the following is not a risk of having a weak password?

A. Financial loss

B. Identity theft

C. Downloading a virus

D. Compromised sensitive information

You should always change your passwords every three months.

A. True

B. False

Do you remember the password that you just created?

A. Yes

B. No

Which of the following is NOT a good way to remember your password?

A. Using a secure password manager.

B. Using first letter from each word in a sentence, a phrase, a poem, or a song title.

C. Writing them down and keep them in a securely locked place.

D. Writing them down on a post-it note on your monitor or under your keyboard or mouse pad.

DQ Pro

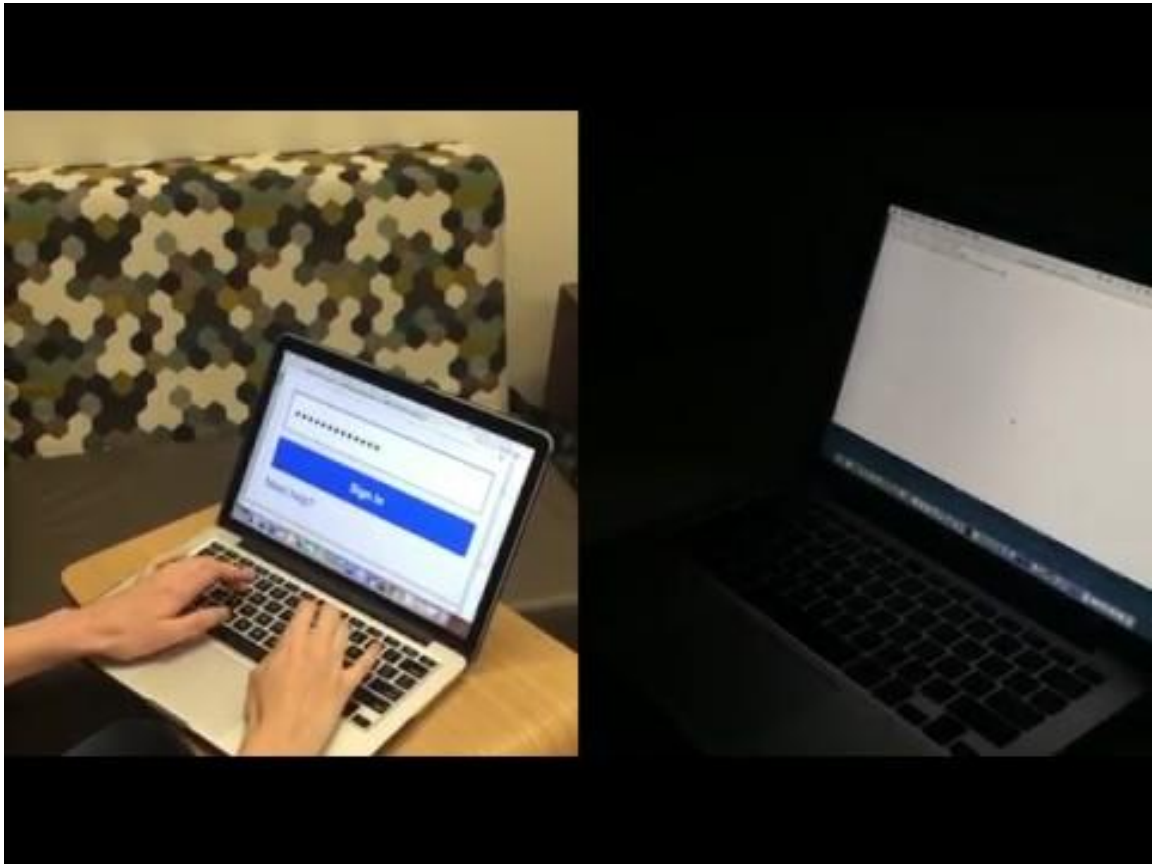
Module 1: Security & Data Protection

Section 2: Malware

How a simple download can lead to destruction and a data breach for the company

Essential Questions

1. What are the risks involved with malware to you and your company?
2. What are different types of malware?
3. What are some signs that your device is infected by malware?
4. How do you protect yourself from malware and remove it from a device once it is infected?



link for video
https://drive.google.com/file/d/0BxV7DNxRPfzFMTRnR0xhcmlDNEk/view?usp=sharing

What is Keylogging?

Keylogging is the process of secretly recording keystrokes by an unauthorized third party.

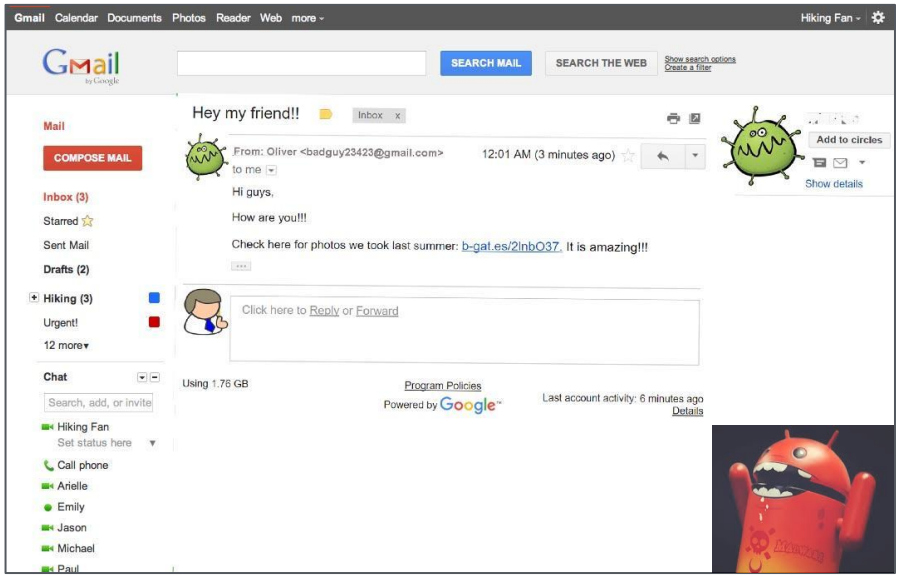
Keyloggers present no threat to the system itself. However, they can pose a serious threat to users, as they can be used to steal usernames, passwords, credit card details and other confidential information entered via the keyboard. As a result, cyber criminals can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, user names, email passwords etc.

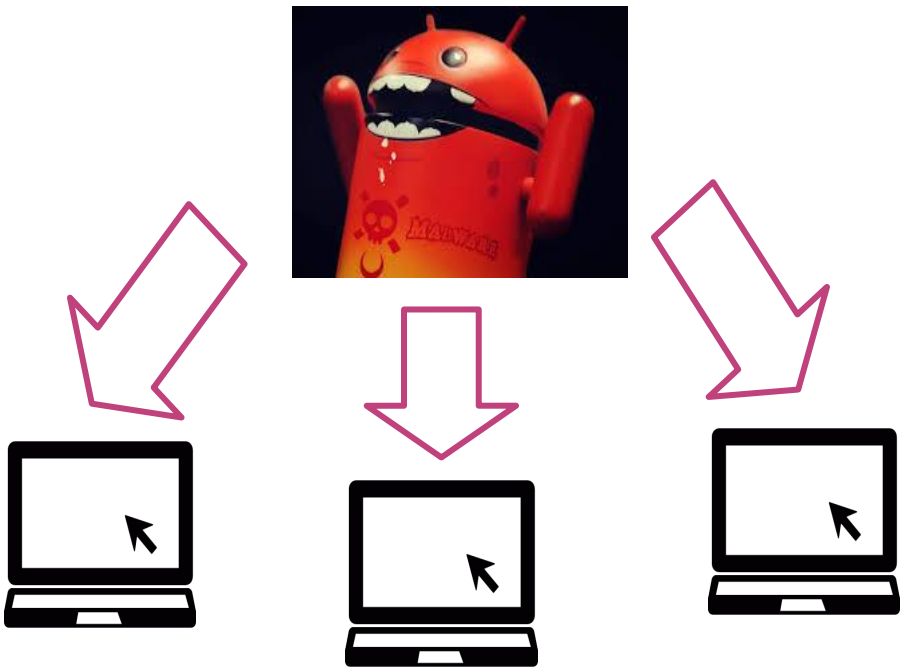
Is keylogging scary? Actually, keylogging is only one of the many **malware** around your life!

Malicious Soft**ware** → Malware! What *is* that?

Malware is used to describe viruses, adware, any software that is used to harm a unsuspecting user. Malware is a general term for malicious software. Malware includes viruses, adware, Trojans and spyware. Many people use the terms malware and virus interchangeably.

Why it is important to protect the company and yourself from these threats? What if the computer in the company are infected with malware?





As companies increasingly turn their businesses online, malware is on the rise and becomes more sophisticated. According to 2015 Cyberthreat Defense Report, over 70 percent of organizations report been compromised by a successful cyber attack in the year of 2014 and the average cost of data breach in one company has increased to $3.5 million.

The pervasiveness of malware can lead to severe security issues for you and your company, including

- **stolen password**
- **damaged devices**
- **financial loss**
- **damage to reputation**
- **data breaches**
- **customer information or intellectual property (IP)**

Other types of Malware

click on the name to find out more!


Keylogging

Virus



Spyware

Adware



Zombies

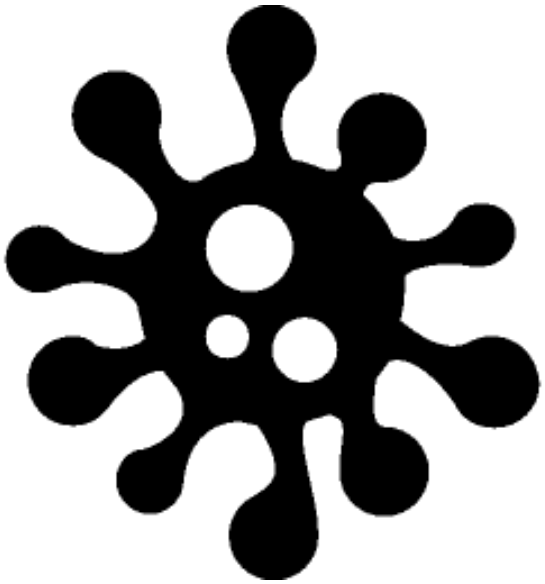
Botnet



Ransomware

Browser Hijacking


"Hola, I'm a Virus."



We are malicious computer programs that can spread to other files. Our effects include displaying irritating messages, stealing data, or giving hackers control over your computer. We can exploit security flaws in your computer's operating system to run and spread automatically.
We can infect your computer in various ways, including via an email attachment, in a download from the Internet, or on a USB drive.

DQ Pro

"Hello, I'm Spyware."

I am the software that permits advertisers or hackers to gather sensitive information *without* your permission.

You can get spyware on your computer when you visit certain websites. A pop-up message may prompt you to download a software utility that it says you need, or software may be downloaded automatically without your knowledge.

When I installed on your computer, I can track your activity such as the websites you visit. I then report it to unauthorized third parties, such as advertisers. In addition, I consume memory and processing capacity, which may slow or crash your computer.

"Hi, I'm a Adware."

I display advertising banners or pop-ups on your computer when you use an application.
So I am not necessarily bad.
In fact, the advertising can fund the development of useful software, which is then distributed free.

BUT I would be harmful if

- I am installed without your consent
- I install myself in applications other than the one it came with and displays advertising when you use those application
- Hijacks your web browser in order to display more ads (see my brother Browser hijacker)
- Gathers data on your web browsing without your consent and sends it to others via the Internet (see Spyware)
- I am designed to be difficult to uninstall

I am an infected computer that is remotely controlled by a hacker and I am part of a large group of compromised computers called a botnet. Once a hacker can control your computer remotely via the Internet, your computer becomes a zombie.
I am commonly used to send spam, launch denial-of-service attacks and infect other systems.

"Hi, I'm a Zombie."

"Hi, I'm a Botnet."

I represent a bunch of infected computers that are controlled by a hacker for malicious purposes.

For example, a spammer can use me to send out spam email. In fact, the majority of all spam is distributed this way. This allows spammers to avoid detection and get around any blacklisting applied to their own servers. It can also reduce their costs because the computer's owner is paying for the Internet access.

Hackers can also use botnets to launch a distributed denial-of-service attack (DDoS). They arrange for thousands of computers to attempt to access the same website simultaneously, so that the web server is unable to handle all the requests reaching it. The website thus becomes inaccessible.

I deny you access to your files or computer until you pay a ransom. Malicious software can hold your data hostage. For example, the Archives Trojan copies the contents of the My Documents folder into a password-protected file and then deletes the original files. It leaves a message telling you that you require a 30-character password to access the folder, and that you will be sent the password if you make purchases from an online pharmacy.
Some criminals use asymmetric or public-key encryption so that the password is not easily recoverable.

"Hi, I'm a Ransomware."

"Hello, I'm a Browser Hijacker"

I change the default homepage and search engine in your Internet browser without your permission.
You may find that you cannot change your browser's homepage once it has been hijacked. Some hijackers edit the Windows registry so that the hijacked settings are restored every time you restart your computer. Others remove options from the browser's tools menu, so that you can't reset the start page.
I am used to boost advertising revenue, as in the use of blackhat Search Engine Optimization (SEO), to inflate a site's page ranking in search results.

I can be very tenacious, as well as sneaky. Attackers use clickjacking, also known as a UI redress attack, by inserting multiple transparent, or opaque, layers on a webpage.
This technique can trick a user into clicking on a button or link on a page other than the one they were intending to click on. Effectively the attacker is hijacking clicks meant for one page and routing them to other another page, most likely owned by another application, domain, or both.

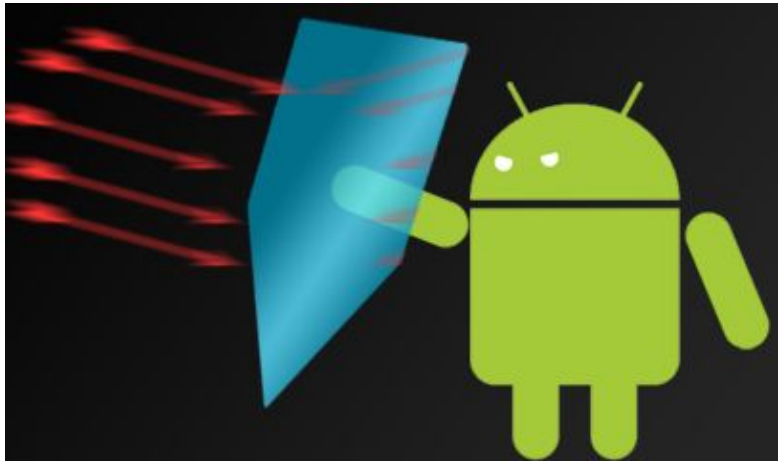
How do you know your computer is infected?

You should check me if I have:

- Slowed-down performance
- Lots of popups
- Unusual network connection
- Running out of hard drive space
- New homepage
- Disabled security protection
- Crashes

Best practices for internet browsing:

- Keep your browser up to date
- Turn on your browser popup blocker
- Install ad-blocker extension on your browser
- Install anti-virus software and firewall
- Scan files before downloading
- Use HTTPS, which means the website is employing SSL encryption.



Which of the following is **NOT** a potential risk of malware to your company?

A. Data Breach

B. Financial Loss

C. Stolen Password

D. Drop in stock price

E. Damaged Reputation

In order to protect against keylogging, which of the following is NOT a good choice?

A. Changing password frequently.

B. Installing anti-virus software or use firewall on the laptop.

C. Download only from trusted sources.

D. Consider switching browsers.

DQ Pro

What may NOT be signs that your laptop is infected by Malware?

A. Homepage was changed without your consent

B. Your system crashes or does not work properly

C. Constant popup windows on your computer

D. Official updates from your browser

DQ Pro

Identify which of the following are NOT good practices when browsing the internet?

A. Use HTTPS, which is safer

B. Download files as long as they are sent from friends

C. Install anti-virus software and turn on the firewall

D. Update your browser from time to time

Drag each term into the category that best describes its effects on the user.

Spyware | Spam | Spoofing | Adware | Virus | Keylogging | Ransomware | Phishing | Zombies

Damaged hardware

Data breaches

Bad user experience

DQ Pro

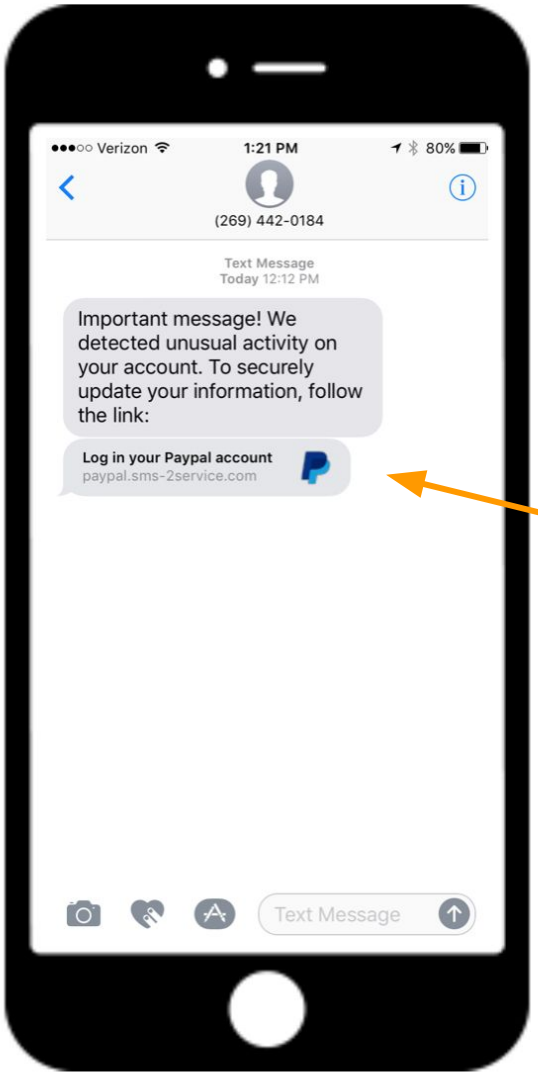
Module 1: Security & Data Protection

Section 3: Communication

What you need to know to stay safe

Essential Questions:

1. What is social engineering? What are types of social engineering?
2. What potential harm can it cause to your company?
3. What precautions should you take when sending and receiving company email?
4. What precautions should you take when using social networking sites?



Do you click on this link?

Do you enter your login information, or close the window?

techihuahua.org.mx/account-updating-information/websc-login.php?Go=_Restore_Start&_Acess_Tooken=fa6bb3e989cbaf13ab4a83d7c0084b30fa6bb3e989cbaf13ab4a8

Sign in to SAIS | WhatFont | Bookmarks | App Suite. Login | Undervalued Stocks | Customer Log In | Box | COL Financial - Philip | AEST to Philippines | Other bookmarks

Log in to your account

Email address

Password

Log In

Forgot your email address or password?

Sign Up for Free

All in one pay.

Pick a card, any card, or bank account, or even apply to get a line of credit from us. It's your money, you choose how to spend it.

Simple. And usually free.

It's free to sign up for a PayPal account, and we don't charge you a transaction fee when you buy something, no matter how you choose to pay.

About PayPal | Contact Us | Fees | PayPal Developers | Merchant Services | Worldwide | Site Feedback

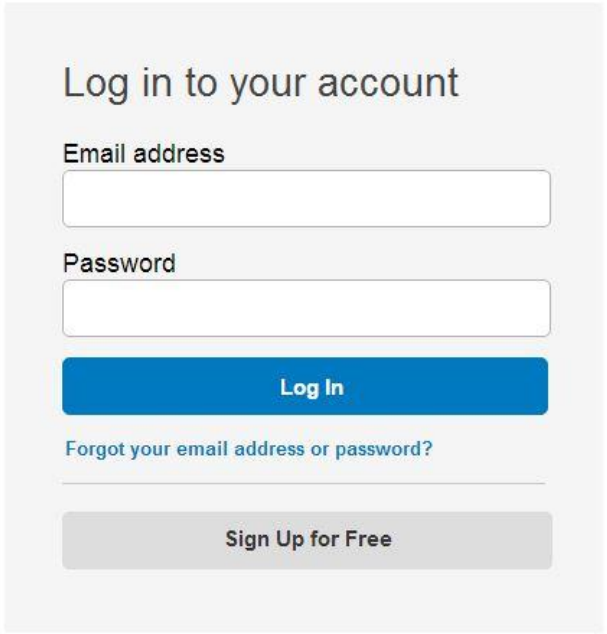
Privacy | PayPal Blog | PayPal Labs | Jobs | Legal Agreements | Site Map | eBay

Be Careful!

techihuahua.org.mx/account-updating-information/websc-login.php?Go=_Restore_Start&_Acess_Tooken=fa6bb3e989cbaf13ab4a83d7c0084b30fa6bb3e989cbaf13ab4a8

Sign in to SAIS | WhatFont | Bookmarks | App Suite. Login | Undervalued Stocks | Customer Log In | Box | COL Financial - Philip | AEST to Philippines | Other bookmarks

1. Wrong Paypal Website Address



All in one pay.

Pick a card, any card, or bank account, or even apply to get a line of credit from us. It's your money, you choose how to spend it.

Simple. And usually free.

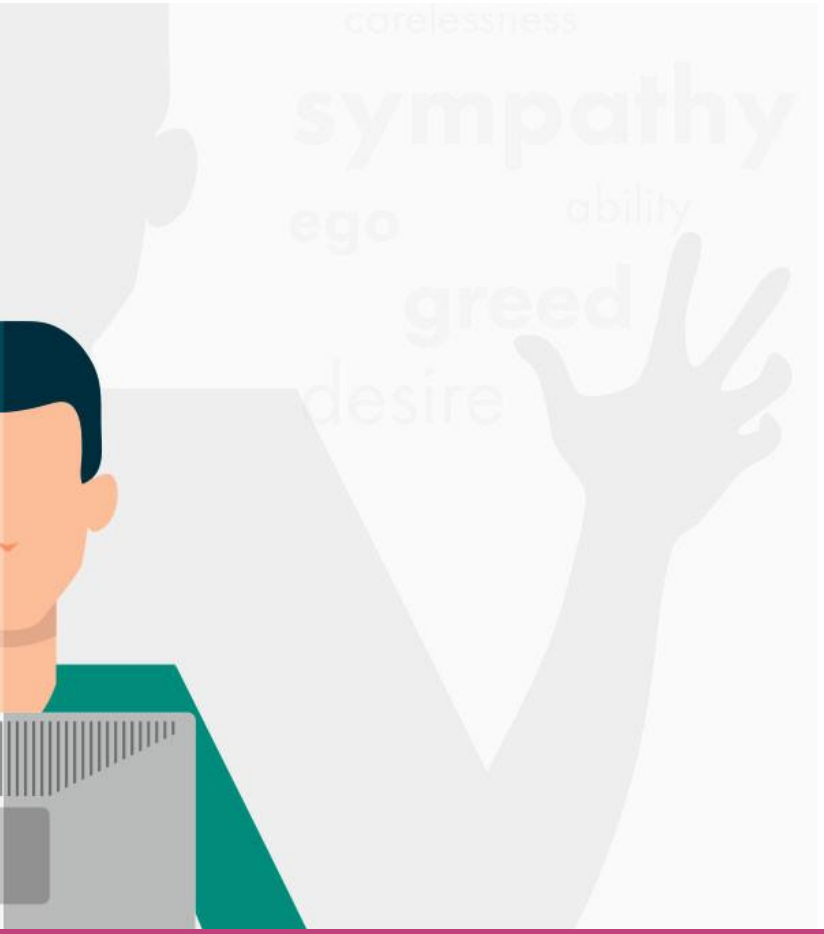
It's free to sign up for a PayPal account, and we don't charge you a transaction fee when you buy something, no matter how you choose to pay.

About PayPal | Contact Us | Fees | PayPal Developers | Merchant Services | Worldwide | Site Feedback
Privacy | PayPal Blog | PayPal Labs | Jobs | Legal Agreements | Site Map | eBay

2. Unclickable Links

Copyright © 1999-2015 PayPal. All rights reserved.

3. Wrong Copyright Information

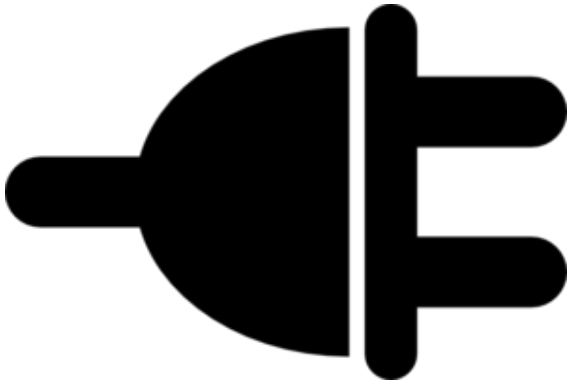


What is social engineering?

Social engineering refers to the methods attackers use to deceive victims into performing an action. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

Many social engineering efforts are focused on tricking users into disclosing usernames or passwords, allowing attackers to send messages as an internal user to further their data stealing attempts.

For example…



In August 2013, malicious hackers distributed emails that simulated the messages Facebook sends when a user is tagged in a post. The links in the messages led to sites that recommended installing a plugin to view the videos supposedly posted on Facebook. The plugin was, in fact, malware designed to steal saved passwords and hack into users' Facebook accounts.

Social Engineering can cause harm to you and your company...

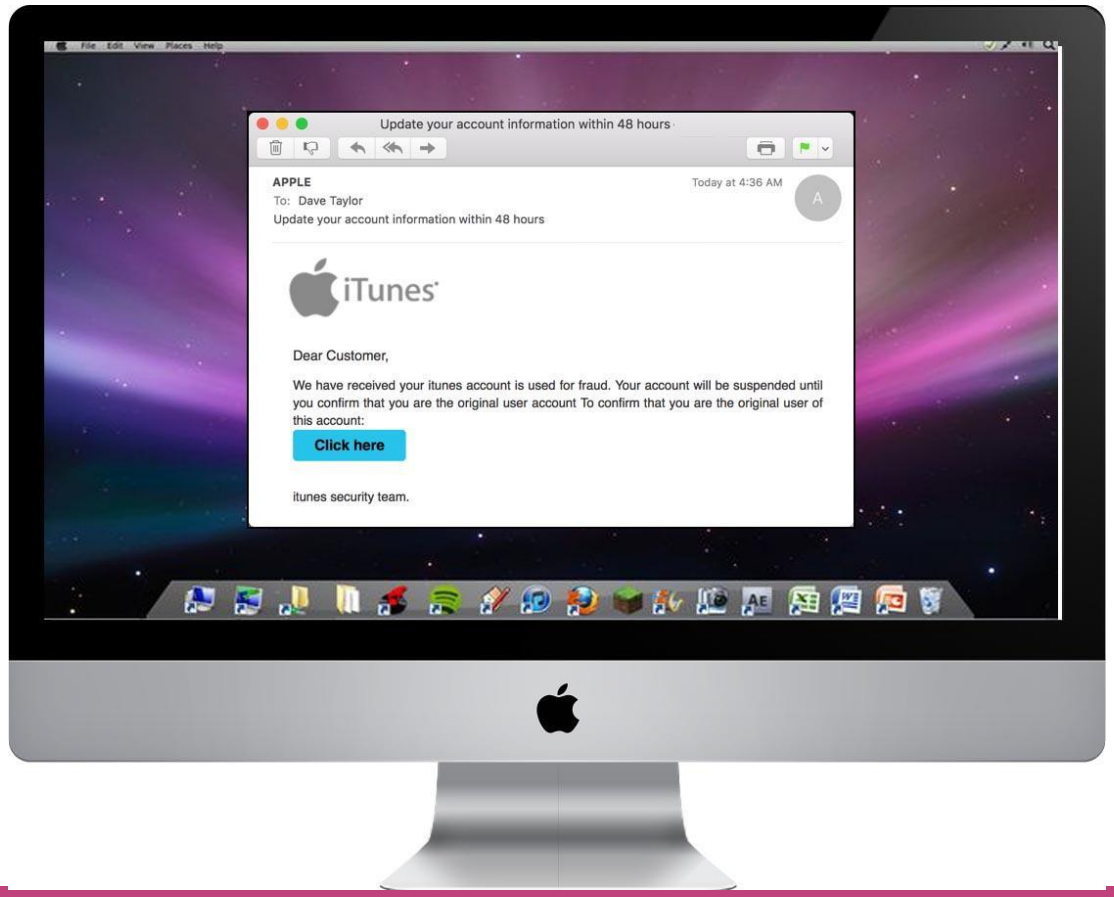
financial loss

stolen data

malware

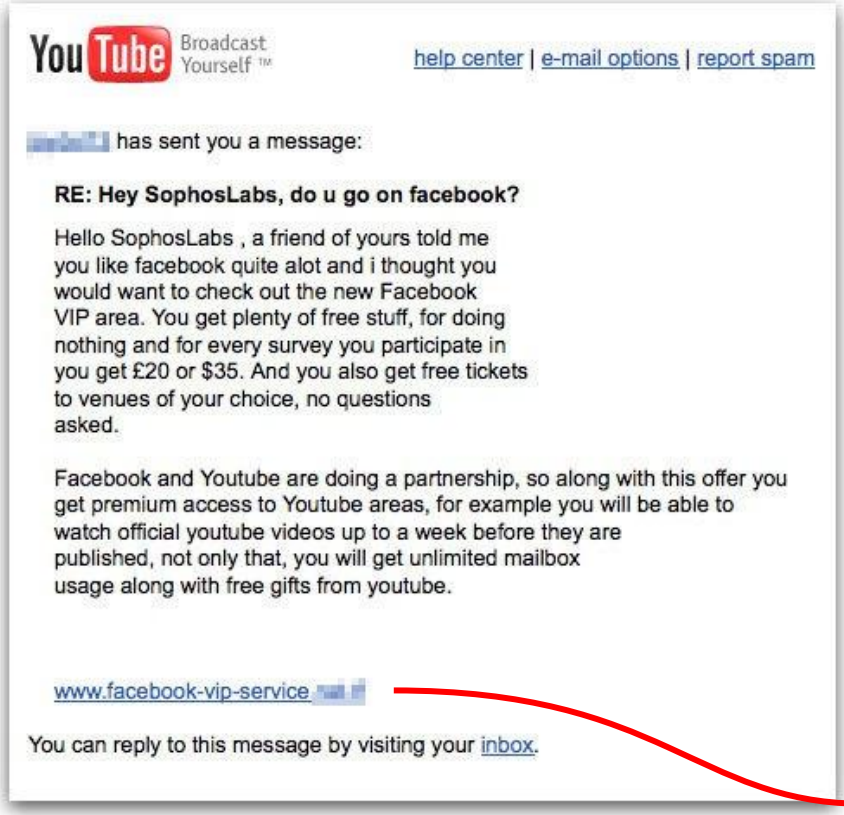
access to assets

Have you ever received an email like this?



Official Update?

Or this?



Website VIP?

*Notice how the url is not facebook.com. This a red flag that this may be a malicious email.

The preceding emails were examples of phishing...

Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party.

Typically in a phishing email scam, you receive an email that appears to come from a reputable organization, such as banks, social media, online games, online services with access to your financial information, or departments in your own organization.

To protect against phishing attacks...

It's good practice NOT to click on links in email messages. Instead, you should enter the website address in the address field and then navigate to the correct page, or use a bookmark or a Favorite link. Phishing emails may also include attachments, which if opened can infect the machine.

Anti-phishing software can block many phishing-related emails.

Another type of social engineering is spoofing.

Email spoofing is when the sender address of an email is forged for the purposes of social engineering.

Phishers (criminals who trick users into revealing confidential information) use spoofed sender addresses to make it appear that their email comes from a trusted source, such as your bank. The email can redirect you to a bogus website where your account details and password can be stolen.

Phishers can also send email that appears to come from inside your own organization, asking you to change your password or confirm your details.

Criminals who use email for scams or frauds can use spoofed addresses to cover their tracks and avoid detection.

From: “Shaynah Browne” <shaynah.browne@einstein.yu.edu>
Subject: message from administrator
Date: Fri, 26 Feb 2016 18:31:11 +0000

Attention;
There’ve been an automatic security update on your Email Account.Click here to login and complete update
http://clinicadeodontologia.com.br/inbox/reset/
Please note that you have withing 24 hours to complete this update. because you might lose access to your Email account

Email spoofing can sometimes mimic the tone and instructions of an administrator in your own network.

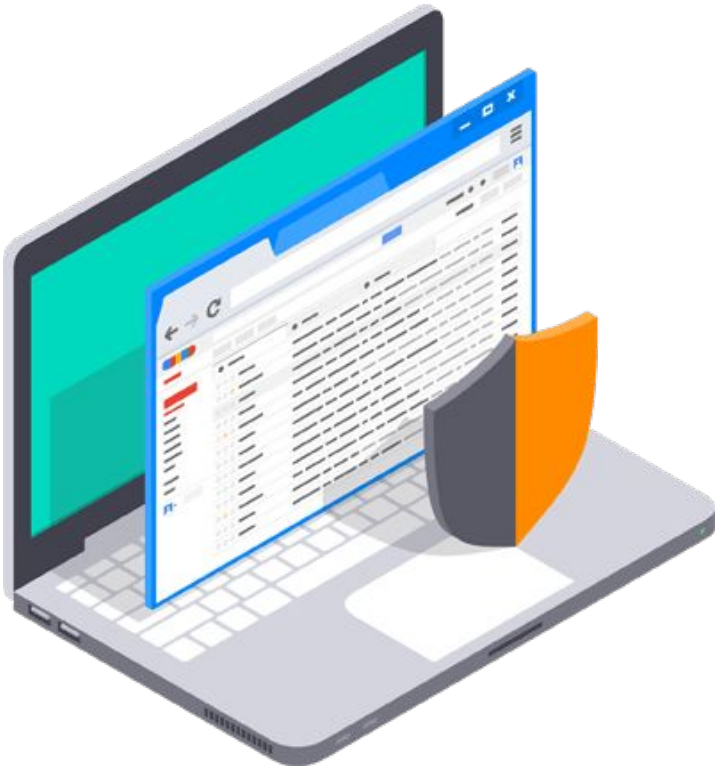
Make sure that you are familiar with the email addresses of your network administrators so that you are not tricked into giving information to a scammer.

Email etiquette... it's not just about being polite, it's about keeping you safe.

On average, 28% of the work-week is spent reading, writing, and responding to email- that's about 650 hours a year *. Therefore, knowing basic email etiquette is more important than ever.

Perhaps the most important rule when it comes to email in the workplace is **NEVER** use your personal email for **ANY** work correspondence. Companies have security tools designed to keep emailing safe, using your own account bypasses these safety measures and puts company information at risk, In addition, using a personal email account can also put your job at risk..

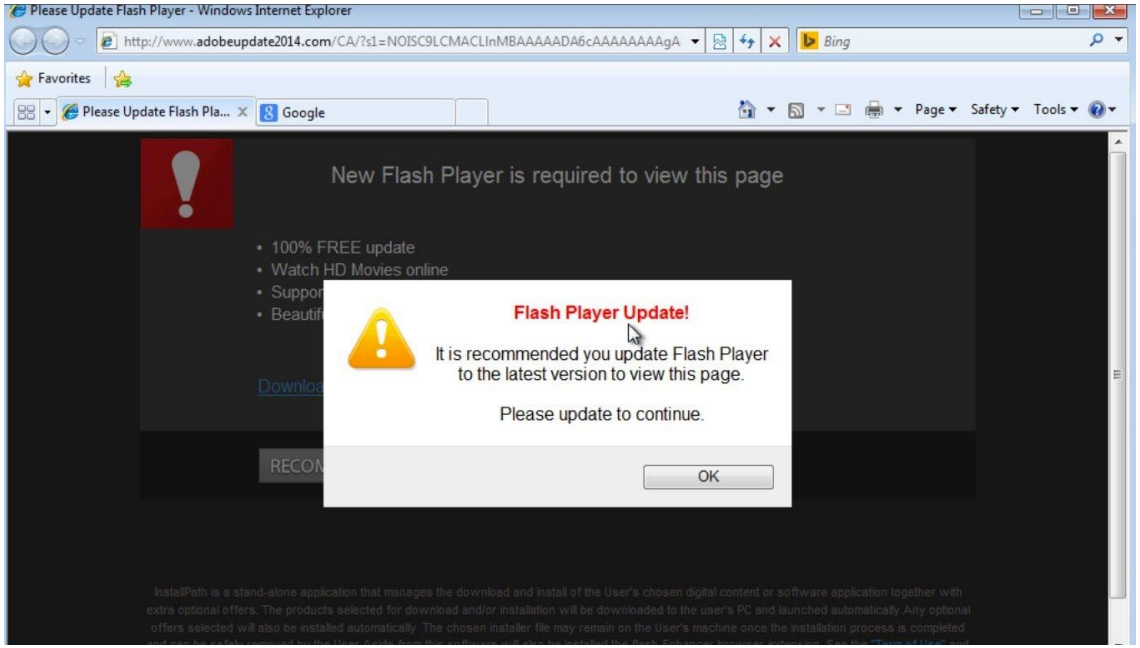
* From McKinsey Global Institute and International Data Corporation 2012 report
https://img.washingtonpost.com/rf/image_1484w/2010-2019/WashingtonPost/2012/07/31/National-Enterprise/Images/mckinseygraphic.jpg?uuid=6T6O8NshEeG4Kcq3hjOvfA



Some other things to remember when sending work correspondence via email:

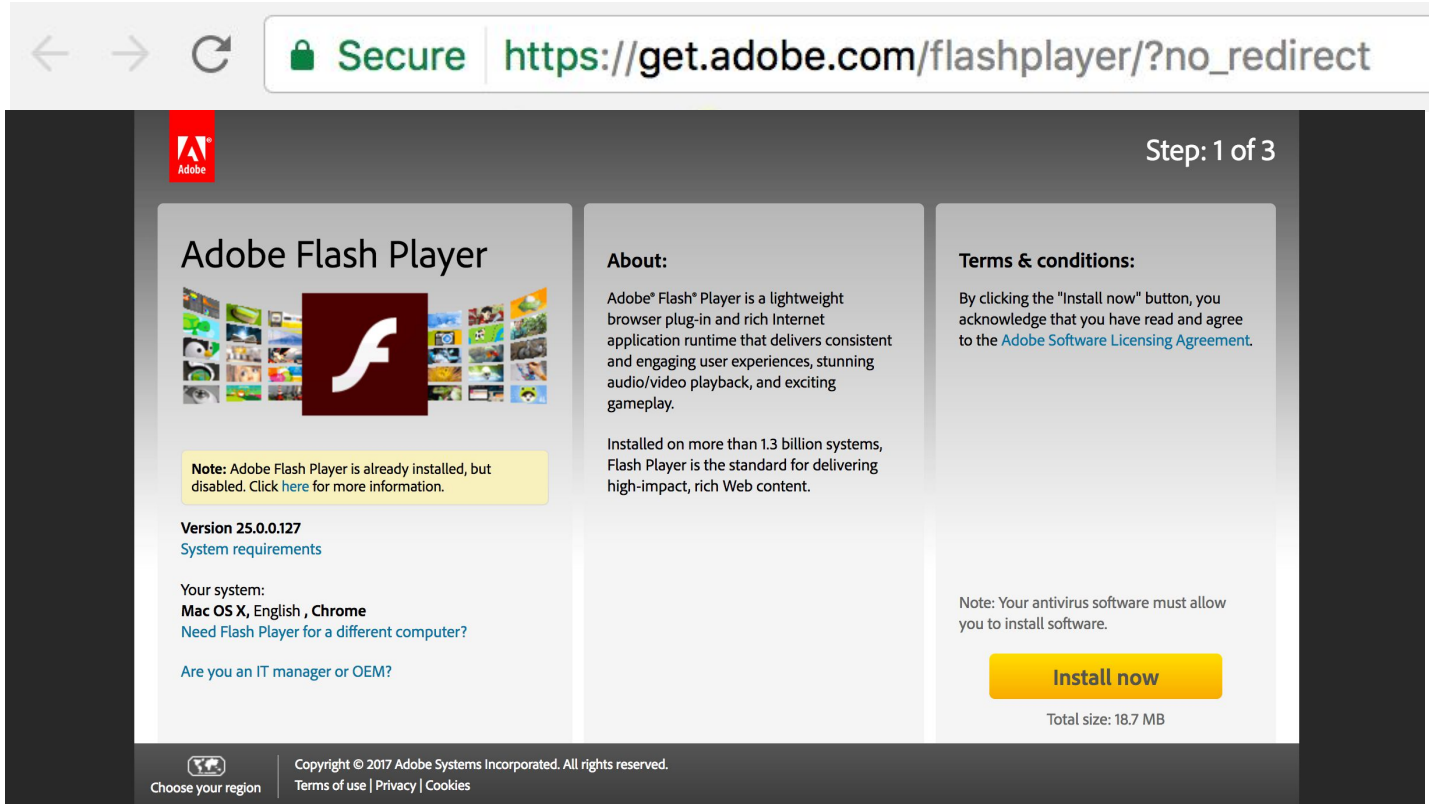
- No adding ccs unless you ask and know the person. This can give cced people the ability to add themselves to other lists and access important information
- Don't talk to strangers - these could be social engineering scams.
- Always scan email attachments before downloading them onto your computer.
- And remember that nothing is 100% confidential, so always err on the side of caution when writing work emails.

Can social engineering target me outside of email?



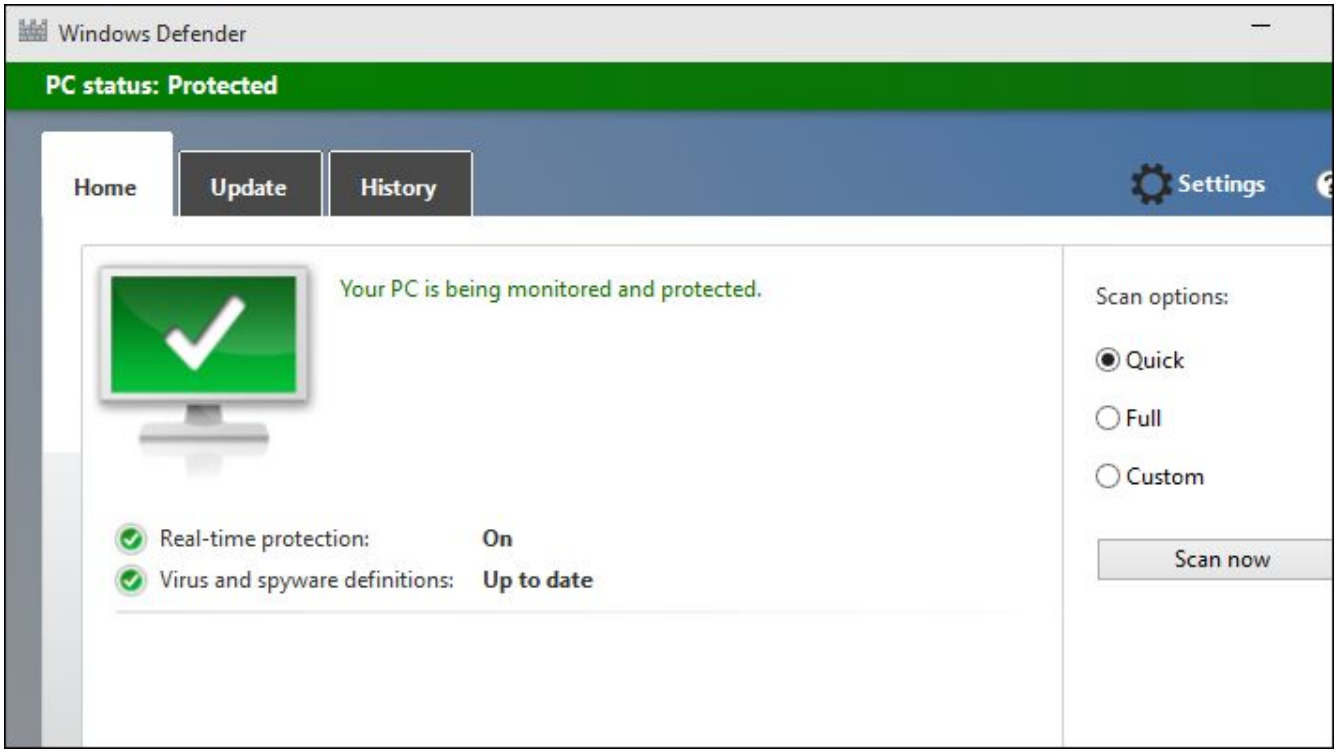
The oldest trick in the book….Flash updates. These prompts are amongst the most common malware scams. One scam in particular, the Flashback Trojan Horse, infected over 600,000 Macs.

How do you prevent? Ignore all prompts for Flash updates. Regularly update Flash by checking Adobe's website: get.adobe.com/flashplayer



The second oldest trick…browser popups telling you that your computer is infected. Browser based applications cannot scan your computer for viruses. This is also a scam.

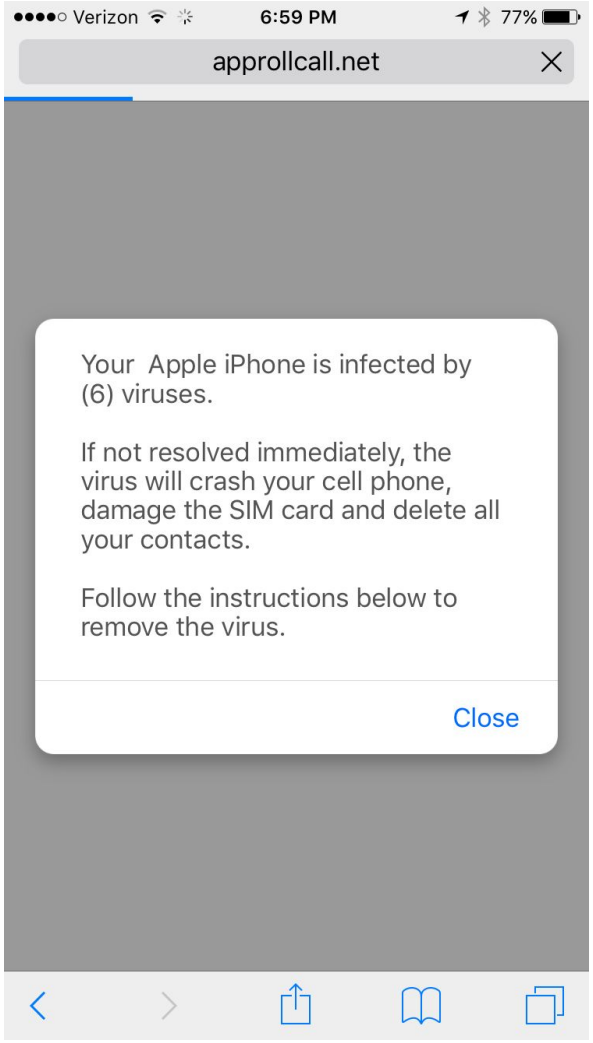
The only official notification of viruses will happen outside of the browser, through a built-in program like Windows Defender or an anti-virus software that your company may have installed.



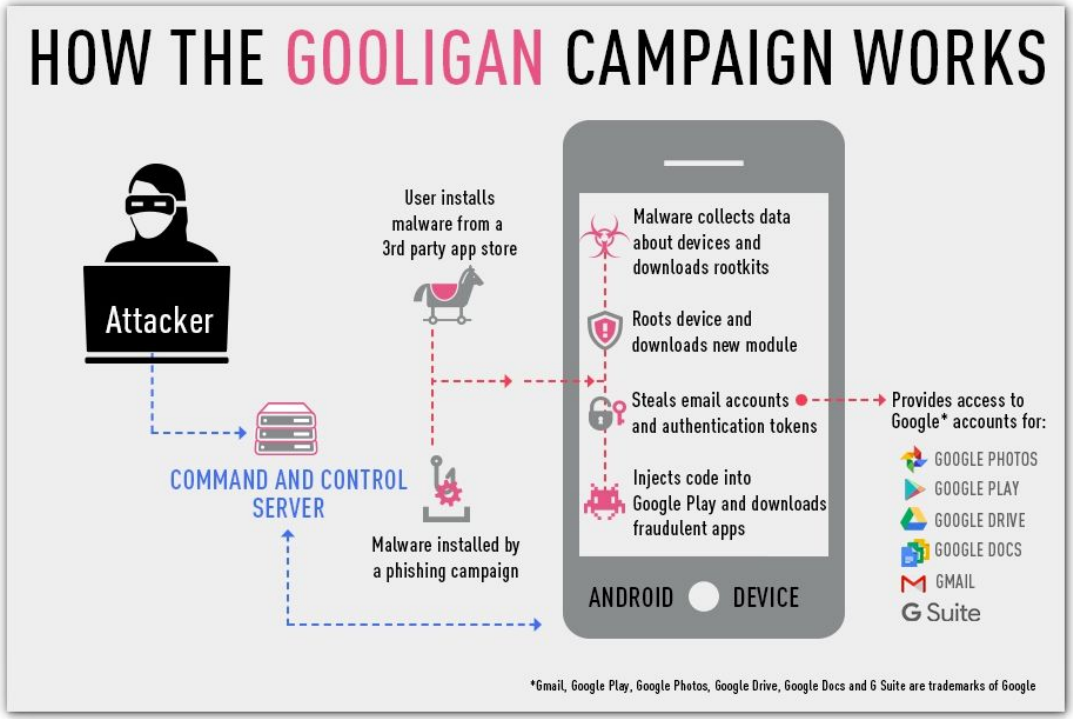
Your desktop or laptop is the only way that you can be infected with malware. This browser pop up occurred while using the iPhone Safari browser.

All security updates are handled through official Apple updates. Apple does not allow third parties to manufacture antivirus software, so you should assume that a message from an iPhone antivirus software company is malware.

Here is another example of a mobile iPhone scam. It could be a portal for ransomware or malware, or a phishing scheme! The "instructions" most likely involve entering a specific password
or entering your credit card information.



Android malware attacks can be even more sophisticated due to the nature of the operating system. Beware of third party applications that are downloaded outside of Google Play.



A third type of social engineering are hoaxes, which are reports of false and unsubstantiated claims, in an attempt to trick or defraud users.

A hoax could be an attempt to solicit money, an attempt to install malware, or an attempt to consume bandwidth (by having users forward a hoax email).

Hoaxes in the form of emails do some or all of the following:

- Warn you that there is an undetectable, highly destructive new piece of malware
- Ask you to avoid reading emails with a particular subject line, claiming it contains malware
- Claim that the warning was issued by a major software company, Internet provider or government agency
- Claim that the malware can do something improbable
- Urge you to forward the warning
- Claim that liking a story or individual on Facebook can result in financial windfalls, charitable contributions and free prizes

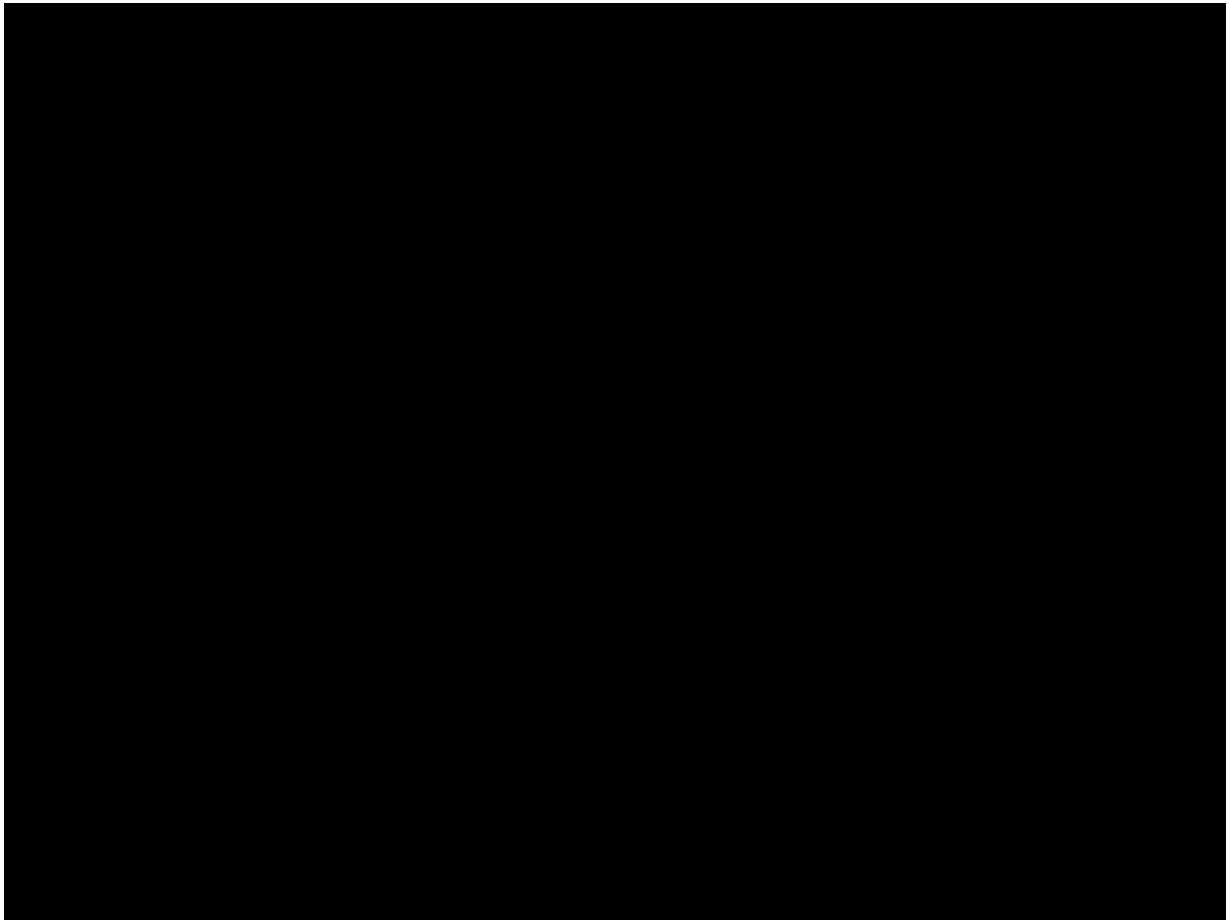
Many users forwarding hoax emails can cause a deluge of email, which may overload mail servers. It's important not to contribute to this by forwarding these emails to anyone in your network. Also, hoax messages may also distract from efforts to deal with real malware threats.

If you've received an email you think may be a hoax, you can simply type the content from the subject line into a search engine; it's likely that others have received this email or something similar and it has been flagged. If an email looks like a hoax but is from someone you know, contact the sender outside of email and ask. Overall, it's best to be cautious… If it looks like a hoax, it probably is.

Social networking websites allow you to communicate and share information…

But they can also be used to spread malware and to steal personal information.

Social networking sites, such as Facebook and Twitter, continue to grow in popularity as attack vectors. Unscrupulous individuals can use information you post online to learn details about you that can be useful for social engineering or guessing the answers to security questions on other websites. Attackers may also compromise an account of a friend and use it to distribute malware or other malicious content.



Link for video
https://drive.google.com/file/d/0BxV7DNxRPfzFMHlvdVJiT3IxWFE/view?usp=sharing

How do I stay safe while using social networks?

Be cautious about what links you click on. Make sure any computer you use to connect to the site is protected with the latest security software and patches. Use strong passwords and use separate passwords for each account. Take advantage of two factor authentication, if available. Be thoughtful about what you post online, and use available privacy settings to limit who can see your information.

Which of the following is not a method of social engineering?

A. Phishing

B. Hoax

C. Spam

D. Spoofing

DQ Pro

What of the following is an example of the harm caused by social engineering?

A. Financial loss to the company

B. Sensitive company information being stolen

C. Downloading a virus

D. All of the above

DQ Pro

When it comes to work email, you should **always…**

A. Scan every attachment before downloading

B. Use your work email address

C. Make sure you know who you are CCing

D. All of the above

You don’t need to scan email attachments received from people you know.

A. True

B. False

Match the following vocabulary with its correct definition.

Email Spoofing	Deceiving recipients into sharing sensitive information with an unknown third party
Phishing	Reports of false and unsubstantiated claims, in an attempt to trick or defraud users.
Spam	When the sender address of an email is forged for the purposes of social engineering.
Social Engineering	Unsolicited bulk email, the electronic equivalent of junk mail, that comes to your inbox.
Hoax	The methods attackers use to deceive victims into performing an action.

When using social networking sites you should never post company specific information.

A. True

B. False

DQ Pro

Module 1: Security & Data Protection

Section 4: Protection Measures

How to keep your device and your information safe

Essential Questions

1. What precautions can you take to protect the data on your devices?
2. What precautions can you take to digitally protect your devices?
3. What precautions can you take to physically secure your device?

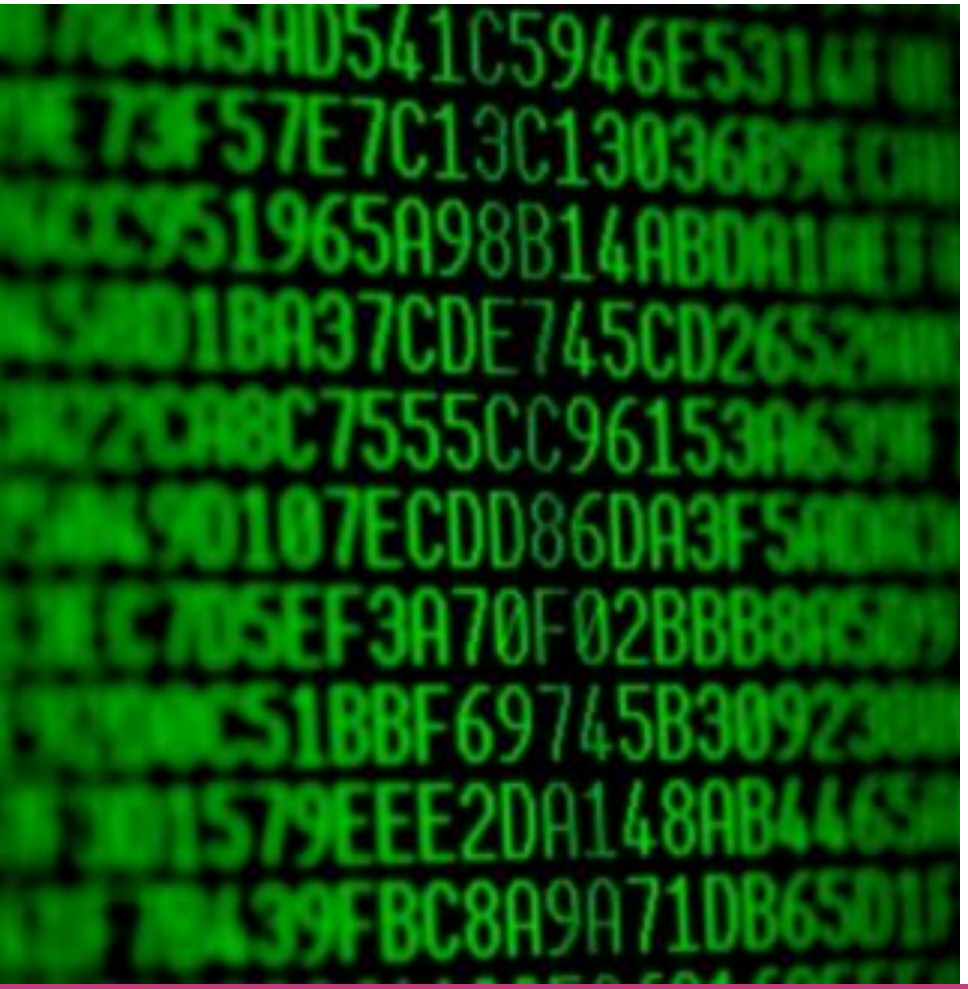
Keep your data secure!

Backing up your files is a great habit to develop.

The process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event, such as a virus that leads to a computer crash.

There are many different types of storage devices you can use to backup your computer, including:

- thumb or flash drive
- external hard drive
- cloud-based services
- writable DVD/CD
- SD card
- data server



Another way to keep your data safe is through encryption…

Encryption is the process of converting information or data into a code, especially to prevent unauthorized access.

There are many different options when it comes to encryption, so it's best to check with your IT Department to see what the company's practices for encryption are. However, encrypting sensitive files, even personal files, is always a good idea.

Did you know?

The secure version of Hyper Text Transfer Protocol (HTTP) is Hyper Text Transfer Protocol **Secure** (HTTP**S**). You've probably seen both of these acronyms before in a web address.

The data being sent between your browser and any website is encrypted only on HTTPS sites. Though it's most likely that websites that gather important data, such as your credit card number or banking information, use HTTPS, it's important to keep this in mind and look out for the 'S' when dealing with sensitive data.

The risks of sharing flash drives...

Viruses can be written such that they will use flash drives to transfer themselves to other computers. It's actually a very common mechanism for some forms of malware to infect other machines. It's important to understand that when you transfer a flash drive from one machine to another, you may very well be carrying malware with you.

To keep data safe, it's important to keep your device safe.

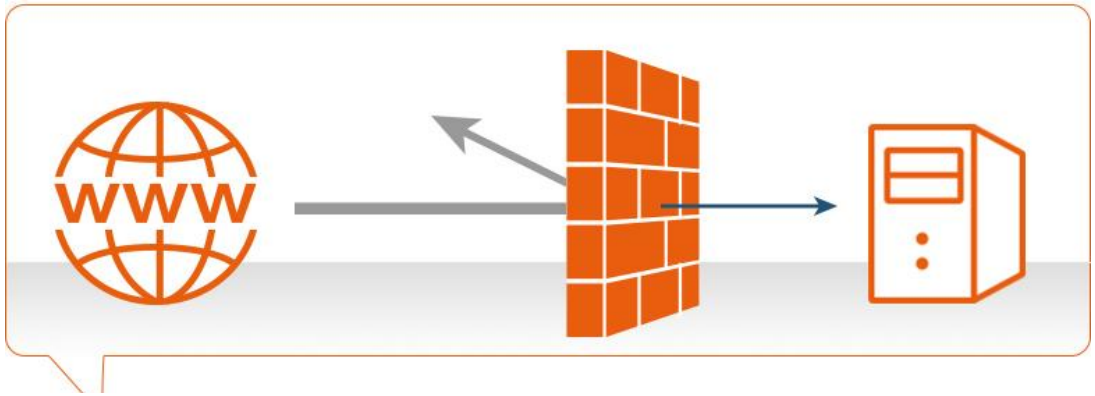
Here are three important ways to do this :

1. Install anti-virus software
2. Set up firewall
3. Install patches on your computer

Anti-virus Software

Antivirus software works like a shield to protect your computer from the malware family, including viruses and Trojan horses, and removes malicious programs like adware and spyware. There is free antivirus software available for general detection and also more robust software for purchase. Be sure to pick the right one to protect against potential threats to your company and you.

Check with your IT Department for recommendations.



Firewalls

A Firewall can be a network security program or a piece of hardware which monitors incoming and outgoing network traffic and then decides whether to block specific traffic based on predetermined security rules.

Check with your IT Department for recommendations.

Patches

Patches are software add-ons designed to fix software bugs, including security vulnerabilities, in operating systems or applications. Patching for new security vulnerabilities is critical to protect against malware. Many high-profile threats take advantage of security vulnerabilities. If your patches are not applied in a timely manner or are not up to date, you risk leaving your computer open to hackers.

There are several rules to remember to help keep your device safe in a public space.

- Don't ever leave your device unattended. If you have to, in your car for example, make sure you hide it.
- Use passwords on your devices to protect your privacy. You should also use passwords for specific, confidential files you keep on your devices.
- Keep only documents you need on your device. Remove the older files you don't need after storing them on an external drive.
- Don't allow automatic filling of a password on your phone. If you do, ANYONE can access your account with your phone.
- If there is an incident that involves a potential breach of confidential information, report it immediately.

Be careful on open public wireless networks

Bad guys can monitor unsecured networks and look for your credit card or personal information. If you have to use public wifi, avoid using sensitive data, personal or corporate accounts while connected.

Remove personal information before discarding used phones

You may store sensitive information like addresses, emails, voicemail, and passwords in your old devices. So, before you discard or dispose them, be careful that they do not fail into the wrong hands.

Step 1: Factory reset your phone
Step 2: Remove or erase SIM cards
Step 3: Double check on the information
Step 4: Discard with care

Which of the following is NOT a way to keep the data on your device(s) secure? Select ALL that apply.

A. Encryption

B. Pop-up blocker

C. Cloud backup

D. Password manager

Match each term on the left with its definition on the right.

___ 1. anti-virus software	A. software add-ons designed to fix software bugs, including security vulnerabilities, in operating systems or applications.
___ 2. firewall	B. a program that can prevent, search for, detect, and remove software viruses, and other malware
___ 3. a patches	C. the process of converting information or data into a code
___ 4. encryption	D. a system designed to prevent unauthorized access to or from a private network

Which of the following are ways to physically protect your device(s)?

A. Use password protection.

B. Do not leave devices unattended.

C. Store devices out of sight when travelling.

D. All of the above.