Click! Game over.

PRACTICAL TRAINING GUIDE

TABLE OF CONTENTS

Who Are the Hackers?

There are a number of different hacker entities in the world; each has their own agenda:

- **Cyber gangs**
  - Motivated by money
  - Steal credit card information, medical records, and personal data and sell in underground markets
- **Hacktivists**
  - Motivated by politics and making a political statement
  - They try to "expose" governments and corporations for various reasons
- **Nation states**
  - Highly resourced, funded, and skilled hackers who work for nation states
  - Motivated by corporate, military, government secrets
  - They steal secrets to help their country close the technological gap with other countries, or give them the upper hand in international business negotiations and disputes
  - They can hack in to your network within minutes, move laterally within hours, and then be hiding in a company's network for months, if not years!
- **Insider threats**
  - Someone working inside your company who could be upset, or vindictive about something, and wants to take revenge on the company
  - They steal data and sell on an underground market
  - Or they delete data to be spiteful
  - May also be an unsuspecting employee who has been socially engineered to allow an outside hacker access to the company network

Targeted Email Phishing

By far the most common form of hacking into companies, and onto your computers, are targeted "phishing" emails. Please read this section many times over, as this is one of THE most important sections of the entire training!

In a phishing attack, the hacker sends you an email that can either:

- Pretend to come from a financial or e-commerce website such as Ebay, Amazon or Paypal
- Pretend to come from people you trust like a friend, your bank, or a government agency
- Suggest that something ***bad*** will happen if you do not provide personal details right away
- Offer you a free prize or award

The emails will normally persuade you to open an **attached file**, or **click on a link to log into** their fake "*website*," so you can change your password, view something, or provide details. Once you visit and log in, it's **Game Over**. They have your username and password, and can also drop *malware* onto your system if they want.

Many times, the bad guys will use details about you, such as your name, what you do, background and preferences (things that don't usually change over time), that they have stolen about you from a large breach e.g. the recent Facebook breach, so that they can try to entice you to click on a link in an email.

Remember: ALL IT TAKES IS 1 CLICK OF YOUR MOUSE TO GIVE THEM FULL ACCESS TO YOUR SYSTEM

By "full access" we mean it is Game Over!

And “Game Over” = hackers can spy on and steal your emails, messages, browsing habits, passwords, files, pictures, webcam footage, microphone audio etc.

The bad guys are hoping you’re being distracted at work/home because you’re multitasking. But they won’t get away with it now after this training! ☺

So remember to pause before you click any link!

Targeted Email Phishing Mitigation

When you receive an unsolicited/unexpected email, always **pause momentarily**, and think about the context around the email coming in. And ask yourself:

- Hey, who is this email *really* from?!
- Why are they asking me to update my details over email?!
- Why didn’t they call me instead if it was *that* important?!
- Why do I need to give this information?
- Is there a safer way to provide the info?

PHISHING RED FLAGS

When you receive an unsolicited email, please pay attention to the following red flags:

“**From**”	Notice the name in the “From” field, and don’t believe it 100% (The “From” field can be spoofed/faked so pay attention) Always treat this field with suspicion! The email could look like it’s coming a friend, family, colleague, business contact, manager or CEO, when it is actually from a scammer
“**To**”	Is it addressed only to you, or other people as well? If others, ask yourself why are *they* in the email?
“Subject”	**Beware of subject lines such as:** • Your Tracking Details! • “*So-and-So”* shared a document with you… • Confirm your identity! • Verify your account! • Update your account! • You must change your password ASAP! • “Wow/OMG/Check This Out!” • Update/download XYZ software • You have won something! • Please donate to XYZ charity! **Ask yourself: what *emotions* do I feel when I see the subject line??** • Do you feel scared? • Do you suddenly feel a bit greedy for an amazing prize? • Do you feel empathetic to help someone? • Do you feel rushed/compelled to act on something? • Does the sender make themselves out to be a person of authority? • Do you feel curious about an unknown invoice or package being tracked?

Be VERY suspicious of any emails that pique your curiosity, make you scared, or make you want to act immediately on something. *These are common social engineering tactics to make you click a link.*

"Salutation"

Does the email address you by your personal name?
Or something impersonal like "Dear Client/Customer/Hello"
If this is a company you do business with, they should know your name!
(Sometimes hackers want their emails to reach as many recipients as possible, so their email will contain a lot of generic wording)

"Content/Body"

Are there spelling or grammatical errors anywhere in the email?
Is there a trusted big brand logo in the email, to trick you into lowering your guard?
Watch for spelling and grammar mistakes as indications of fraudulent emails
Many thieves operate internationally, and their emails have many spelling or grammatical mistakes
Also, no reputable company sends emails with spelling/grammar mistakes!
Any emails from legitimate companies would never include such spelling errors, and always go through some sort of quality assurance process before being sent out to the masses
So treat any "official" emails with a lot of suspicion

Embedded Link

THIS IS *THE* MOST IMPORTANT THING TO PAY ATTENTION TO IN THIS ENTIRE TRAINING SERIES!

NEVER EVER CLICK ON A LINK IN AN UNSOLICTED EMAIL BEFORE CHECKING:

Is there a link/button inside the email they are asking you to click??
Where does the link explicitly say it is going??

- Now hover your mouse over the link, **BUT DON'T CLICK THE LINK!**
  - *You will now see the REAL final link destination!*
  - Either as a popup message in your email client e.g. Outlook
  - Or you can see it in the bottom left status bar of your browser
  - **THIS IS WHERE THE LINK IS ACTUALLY TAKING YOU!**
  - **If the link in the email, and the link that pops up when you hover your mouse do NOT match, be VERY suspicious!**
- Be aware of slight variations in the website spelling
  - e.g. disney.com vs d1sney.com
- Also follow the address link in the email *aaaaaallll* the way to the first **"/"** (forward slash)
  - The website domain name you see before the "/" is the real, final link destination:
    e.g. www.blah.com-blahblah.*evil*.com/...

If the link has a shortened URL link address, that is also a red flag for unsolicited emails pretending to come from reputable companies e.g. Google, or your bank
e.g. http://ow.ly/blahblah
e.g. http://bit.ly/blahblah

Never respond to login/password reset requests sent via email that you did not initiate or expect!

- Treat any email that directs you to click on a link with caution
- Beware if the purpose of the link is to:
  - Provide your Social Security or credit card number

- Confirm your identity
- Verify your account
- Update your account
- Download software

- Never readily give your personal details in any email, ESPECIALLY if the email is unsolicited!
- Legitimate organizations normally **do not** send customers an email with a link to confirm their account or personal details. (And if they do, shame on them!)

If you absolutely must visit the link, personally type the URL address yourself into the browser!

- Pay attention to the URL address of the website you are typing in
- Malicious websites may use a variation in spelling or a different domain
  - e.g. ".com" vs ".net"

Again, if you can help it, never click a link in an email to update or verify anything

- If you have *any* concerns, you really should personally phone the company and **confirm** the purpose of the email in question!

- Contact the business directly, by phone or by walking into the branch store and ask a staff member what is going on:
  - "Hey, do you guys really need to update my profile?!"

==========

VERY IMPORTANT - legitimate businesses and banks will NEVER ask you to click on a link to update your personal details

You should ALWAYS phone the company yourself, or directly type the company's website address into your browser instead. Never trust the link within the email!

==========

- **Attachments in emails**
  - The email/attachment could be from colleagues, strangers, friends, family, or anyone.
    - Be suspicious of any and all attachments!
    - Plain and simple
  - If in doubt, always refrain from opening it!
    - **Even a friend who accidentally infects their own system with malware, can then inadvertently send you that *same* malware, via an automatically generated email**
  - **Always verify the attachment with your friend, family member or colleague:**
    - Call them immediately and ask them, **"Hey, did you just send me an email with [XYZ] attached?!"**

- **Unexpected emails sent by a friend**
  - Many times, the first thing a virus does upon infecting your system is to send itself to every contact name in your address book, as a way of spreading itself rapidly
  - Therefore, it is imperative to scrutinize any emails or instant messages, *even if you recognize the sender!*
    - Call your friend and ask them:
      - **"Hey, did you *just* send me a link via Messenger?!"**
      - **"Hey, did you *just* send me a PDF via email about XYZ?!"**
  - Keep in mind that the *context* of the message is crucial in determining whether it is a benign or malicious message

    - E.g. if your friend and you went camping the past weekend, and she is now sending you a link to your camping pics, it's likely safe to assume she sent the email
    - But if you receive an email from her, with a document you were not expecting, it could be a simple tactic by a hacker to get you to open a malicious document

- **Emails with images**
    - Some malicious emails are presented to the victim as one large *image*
        - But clicking anywhere in the image with your mouse will redirect your browser to a website that will download malware
    - If you do not recognize the email, do not click on these images
    - If not malicious in nature, they are normally just spam, an attempt to get you to buy something
    - Delete them ASAP instead!

If your email provider has the functionality, 100% absolutely make sure you set up 2-Factor Authentication (2FA) to protect your email account (explained in the 2FA section below)

- **If in doubt, at work ask your IT department**
    - **Or type *"email provider* 2-Factor Authentication set-up" into Google and follow the help instructions**
- **Gmail and others have been offering 2FA for many years**

Finally, whenever you hear national news about a new breach at a company that you have done business with, be very paranoid about any new emails that come into your inbox, as oftentimes, the hackers will use this stolen data about you to subsequently social engineer you…

E.g. they will send an email pretending to be from the hacked company, asking you to click a link to supposedly "secure your account details."

Yeah right! It's a scam! Do not trust any such emails, and follow the instructions above to contact the company directly if you have to speak to them.

Tip: If you absolutely must open an email that might be suspicious in nature, it's better to open it on an iPad or iPhone, rather than on a desktop computer (as the iOS is a harder operating system to compromise in general than Microsoft Windows or macOS).

Macro Malware

Put simply, macros are a type of programming code that are embedded inside Microsoft Office .XLS/.DOC/.PPT files, that can perform certain functions to make your job much easier.

Having said that, macros are also GREAT for bad guys trying to deliver evil code to you, because they can be executed with a single mouse-click inside Microsoft Office!

Because the vast majority of Microsoft Office files found on the Internet are malicious, if you receive a Microsoft Office file from the **Internet** or an **untrusted** source, there is a VERY good chance it will contain a ***malicious macro***.

Macro Malware Mitigation

Macros are usually disabled these days by default (in your **Protected View** settings), which turns off most editing functions inside the file. This is GOOD! We want this ☺

- **It protects us from files downloaded from the Internet**
- **Or files received via Outlook from an untrusted sender**

REALLY think hard about whether you need to even enable a macro in a file for anything at all.

- Maaaybe for Excel if you do number crunching
- But not really for .PPT or .DOC files
- **When you're at work, only enable macros inside files stored in trusted locations**
    - If you know the file is from a trustworthy source, and you want to edit, save, or print the file, then you can exit Protected View for that one particular file

The good news is that Microsoft is now explicitly making it hard for end users from enabling Macros, and forcing users to go through several 'hoops' to enable them. This will significantly improve security by closing this attach vector for so many different social engineering scams. Bravo Microsoft

BEC Emails

The goal of "BEC/CEO Fraud" emails is to persuade you to complete a wire transfer – usually to an international bank. These emails will try to entice you based on urgent language, and your relationship with the email sender.

Please remember: there will ALWAYS be a false sense of urgency to pay!

Hackers will specifically target people conducting certain kinds of high-value transactions:

- E.g. people buying houses through a realtor or estate agent
- Or people working in Payroll or Accounts Payable who conduct international wire transfers

Hackers will send the email from a high-level executive's email inbox, **such as your CFO.** Or they will email from a **look-alike company** website domain that is one or two letters different from your actual company domain:

e.g. Pepsl.com instead of Pepsi.com

- You might be contacted using a spoofed email address or phone number
- They might also impersonate your company's suppliers/customers/vendors
- They will also spoof internal documents needed to make a legitimate wire transfer, such as:
    - An overdue invoice
    - An urgent request to complete a payment within a few hours

Real estate companies are also very susceptible to BEC recently, because homebuyers are already preparing to send a large down payment of money.

1. The bad guys will phish an employee's credentials with a targeted phishing email
2. Then log into their inbox and do reconnaissance for a while
3. In the last few days before the house is to be purchased, instructions will be emailed to the homebuyer to change the payment type and/or payment location to a fraudulent bank account

BEC Email Mitigation

By far the easiest way to stop BEC fraud altogether is to make a two-minute call and verify the transaction/invoice/payment request with the supposed sender.

(The phone call serves as a second factor authentication ☺)

ABSOLUTELY AVOID VERIFYING ANY LARGE WIRE TRANSFERS VIA EMAIL!
ALWAYS carefully verify large invoices and payments:

- Never pay unless you know the bill is for things that were actually ordered and delivered
- **Make sure your procedures are very clear for approving invoices**
- **Implement strict international wire transfer policies!**
- Limit the number of people who are authorized to place orders and pay invoices
- Make sure major spending can't be triggered by an unexpected call, email, or invoice
- **Having two people independently authorize LARGE wire transfers is the way to go!**
    - *It's possible for one person to be tricked, but harder for two.*
- **Ideally you want a confirmation call from your bank whenever there is a large wire transfer e.g. via fax communications**
- Whenever possible, set up 2-Factor Authentication for authentication to your bank, company portal and web-based email accounts e.g. Gmail
- If possible, conduct transactions from a non-Windows system, with the bare software essentials and Internet restrictions (please work with your IT department to set this up, if it is feasible in your business environment)
- Check the auto-forwarding rules within your email accounts.
    - If the attackers have access to your email account, they may setup auto-forwarding rules so they can monitor conversations and intervene when a wire transfer is about to happen

NEVER blindly trust your phone's caller ID, as incoming numbers can unfortunately be faked these days
Pay attention to how someone is asking you to pay for something in the email/phone call:

- *If they want you to pay with a wire transfer, reloadable card, or gift card = 100% scam!*
- *NOTE: iTunes Gift cards are becoming VERY popular these days,* because they can quickly earn cash, it's basically irreversible, and also anonymous. Plus they don't need anyone to help them cash out the money

(Finally, if you suspect someone may have access to your email account, check your Sent Items folder, and any Email Rules, to see if there are any suspicious email forward rules set up for your inbox)

Messenger Apps and Smishing

SMS texts and Messenger apps are just as easy to use for social engineering as email. It's just another vehicle for the bad guys to spread their evil malware to you!

Being able to message people using various software and apps is so common these days:

- SMS
- iMessage
- WhatsApp
- Facebook Messenger
- Skype
- Snapchat
- Telegram
- Signal
- LinkedIn

Most people access the Internet via their mobile phones now

- Most emails are opened first on a mobile device

- Due to the smaller screen space on mobile devices, it is harder to see where a presented link will *actually* navigate to if clicked
- It is harder to see the real destination of hyperlinks in emails/messenger apps/SMS
- As a result, people are THREE TIMES more likely to click on a link in an SMS text/Messenger app from a spoofed number, compared to on a computer

BECAUSE OF THESE REASONS - HACKERS LOVE SOCIAL ENGINEERING VIA MOBILE PHONES AND MESSENGERS!

Messengers and Smishing Mitigation

PAUSE!
ALWAYS TAKE YOUR TIME TO ANALYZE BEFORE YOU ACT ON ANY TEXT OR MESSAGE.

- Treat every link presented in an SMS text with intense suspicion
- Don't trust anything that arrives via text/messenger/email, even if it's from your friend, family member or colleague!
    - Remember, emails, texts and phone calls can all be easily spoofed!
    - If you ever receive an unexpected message from a friend/colleague, call them directly and ask them:
        - **"Hey, did you just send me something via text/messenger??"**

No government agency, bank, or legitimate business will ever request personal information via SMS text!

- Never click on any links in unsolicited texts/messages
- Also, never respond to them:
    - Responding verifies that your phone number is active, and they might start bombarding you with malicious messages now as a result ☹

- Be extra vigilant if the message promises:
    - Something free
    - A warning to update or confirm your password or personal details

Vishing

- Vishing = social engineering using voice phone calls
- Because of Voice-Over-IP (VOIP) technology today, it's pretty simple to spoof phone numbers
- Scammers are using vishing to trick you into handing over your money and/or personal and sensitive information by impersonating:
    - Law enforcement
    - Government agencies
    - Big name brands
    - Fake tech support companies

Vishing Mitigation

NEVER TRUST YOUR CALLER ID ON YOUR PHONE. Remember, emails, texts and phone calls can all be spoofed!

Be prepared for vishers to have your **name**, **address**, **phone number** and last 4 of your Social Security Number or credit card on hand (these may have been scraped from previous big company breaches).

*NOTE: Government and tax agencies will **NOT** text, email, or phone you about a debt or default in your account, nor will they threaten you with arrest or prison!*

And if you owe money to the tax agency, you usually won't find out through an email anyway. They will usually send a letter.

If you receive an unsolicited call about tech support, hang up!
(Side note: If you receive a browser popup or ad urging you to call for tech support, ignore it!)

Never give your personal info over the phone when you receive an unsolicited call.

- Even if the caller ID looks good
- **Tell them you will hang up and call *them* back!**
  - (But don't call the number they themselves are providing to you! That number cannot be trusted either)
  - Look up the institution/business number online and call that number instead

Remember: Gift cards are for gifts, not payments!!!
Anyone who calls you and demands payment by gift card (+ asks for PIN) is 100% a scammer!
If you accidentally hand over the gift card details/payment info to the fraudster, call the card issuer (Amazon, iTunes etc.) ASAP and tell them to cancel the card. You may be able to block the scam in time!
(Especially government agencies never demand a specific type of payment)

Finally, there are also certain apps (such as ***MalwareByes, Hiya, Robokiller, Truecaller, and SMS Shield)***, that check incoming calls and texts against a big database filled with scammer numbers, and if they notice a match, the app will block the call or SMS text from coming through.

Ransomware

Ransomware is essentially **digital hostage taking**!

The malware will usually drop onto your system via a malicious link, attachments, or by visiting a hacked benign website.

The malware will then encrypt **ALL** of your important files, making them inaccessible to you!

- We are talking pictures, documents, pdfs, emails. All of it.

Finally, hackers will not decrypt your files unless you pay them a ransom amount, usually in cryptocurrency. Important: If you do end up paying them, they usually come back and encrypt your files *again*, and ask for even more money, as they know you're susceptible to blackmail now ☹

In ***recent years they have also started stealing your data out of your network, to 'add insult to injury', and they will threaten to release all your sensitive data onto the Internet unless you pay up!***

Ransomware is often targeted to:

- Local city government
- Hospitals
- Universities
- Expensive business systems

Ransomware hackers target networks that they KNOW are willing to pay, because the network cannot afford to be *offline* for days or weeks.

Ransomware Mitigation

First and foremost, be extremely careful to follow all the advice in these training modules!

- **Install awesome antivirus software (it should include Machine Learning and Behavioral Analytics)**
- **Make sure your operating systems and all your software are up to date with patches!**
- **Create two backup copies of all of your important and sensitive files:**
  - One can be local, the other in the Internet Cloud (DropBox, Box, Google Drive etc.)
  - Disconnect the local drive from your computer when you are finished backing up your data, so as to prevent ransomware from reaching these files

Your IT and IT Security department will handle most of the above steps for you at work. But if you are ever affected by ransomware at home, please check the following site, as they may host a decryption tool: https://www.nomoreransom.org/

CryptoJacking/CryptoMining

Cryptomining is the use of computing power to perform very difficult mathematical computations, and being rewarded for that work afterwards with cryptocurrency.
Cryptojacking is a theft of your unused computing power to secretly perform that same work!
The hackers want to monetize YOUR computer or mobile phone while it sits idle, instead of buying their own hardware! ☹
So cryptojacking is basically cryptomining, without your explicit permission, with your own computer.

The cryptomining script or code is secretly embedded in:

- Website ads
- Webpages of sites you visit
- Google Chrome extensions and other browser plugins
- Files you download from the Internet or via email
- Google Play Android apps disguised as games, utilities, educational apps etc.
- Public company websites/servers with a lot of computing horsepower
- The code can run in a browser on ANY device!

Remember: the fact that the malicious cryptomining code was dropped onto your system highlights a weak system anyway!

CryptoJacking/CryptoMining Mitigation

The best defense against malicious cryptomining scripts is to use script and ad blockers in your browsers (this is addressed in the Browser Security section).

The latest version of Firefox and Brave browsers can block cryptomining scripts by default.

- **If you use Google Chrome, the browser's *Task Manager*** will show, per tab, how much computing power is being used, so you can determine the website that may have loaded a cryptominer onto your system
    - Use the Task Manager to see which website tab is the one using all the CPU power, and close the browser to stop the cryptomining script from running

Stay vigilant for any signs your system may be running slowly after visiting a certain website, clicking on an ad, opening a file, etc. (although there are certainly other reasons why your machine may slow down).
Note: Detecting cryptocurrency miners can be difficult, because some will throttle the amount of computing power used, or have it run only during specific times of the day or when your system is inactive.

Never click on advertisements
With or without an adblocker, as a security precaution, you should never click on advertisements!

Red Flags

Don't be tough on yourself, social engineering can work on any of us, because we are all human! All the bad guys need to do is find the *trigger* that will make us click a link, or respond how they want us to respond.

Now, let's go over some of the social engineering red flags we keep seeing over and over again in the previous examples:

There are five emotions that social engineers are very successful in triggering:

- Immediacy – Call to action: Is a person or business asking that you immediately do something?
    - *Remember: all 3 types of phishing attacks we discussed have a **"call to action"***
        - TEXT
        - PHONE
        - EMAIL

        They all require an *immediate response!*
- Greed – If you feel a deal is too good to be true, it likely is!
- Fear – Did you receive an email, text, or call scaring the daylights out of you, and persuading you to respond or give up your password or personal information?
- Curiosity – Did you receive a message to track your package, provide shipping details, or confirm information about a flight you didn't purchase?
- Empathy – Is someone asking you for your help, or promising a big reward for a small upfront payment?

Red Flags Mitigation

BE AWARE OF YOUR EMOTIONS!!
When you receive emails, texts or calls, always pause, and think about the context around these messages:

- What is your gut telling you?

Don't give out your personal or financial information to anyone in an unsolicited call, text, or email.
If you ever receive anything from a big-name company or bank, avoid clicking on any embedded links at all costs! Banks should never send you an email or text asking you to click a link and update/supply your sensitive information.

Remember: email addresses, phone caller ID and websites can all be easily spoofed!

Whenever you receive an email or text about something suspicious from a bank or business, do the following:

- Never click on a link in a text or email to visit such a website
- Especially if it is a sensitive site and is asking you to update your password or supply sensitive information
- If you have to, open a separate browser window and, by typing the company website address YOURSELF into the address bar, visit and log in to the company website
- Better yet, call the company and ask them about the message you just received!
- Even better, walk into the company office and ask them!

Search Engine Optimization

Keep in mind that a large number of benign websites are regularly hacked, malicious code is uploaded onto them, and then they appear in Google search results, as a way to get you to visit them.

As a result, one or more Google search results in the first few pages *may be malicious* for the following searches:

- Breaking news
- Natural event
- Celebrity death
- Political news
- "Free" music, software, screensavers, games etc.
- Popular trending topics

Hackers LOVE Google Adwords, and will pay Google to display malicious ads!

"Tech Support Scam" pages are one example that is very popular with Adwords.

Search Engine Optimization Mitigation

First of all, stay away from untrustworthy websites, ESPECIALLY at work!

- It's honestly not worth the risk and bad attention you will receive, if you download something malicious onto your company network

Whenever possible, stay away from sites that supposedly offer ***"free"*** music, software and multimedia (i.e. pictures, videos).

- These links are more likely to contain malware instead

Use bookmarks whenever possible, so you don't need to rely on search results

- Or instead of searching for a website, e.g. Amazon, type "Amazon.com" yourself into the browser

Always be aware of the context on a Google search result link!

- It is important to **scrutinize all Google search results** and ensure that any websites that host the information you seek are relevant websites for *that* type of content
- Assume all Google ads in search results are malicious (until Google has fixed this particular issue)
- If you search for a website on Google, click the top search result: one **that is not an ad!**

After clicking a link in the search results

- It is important to always verify that you have landed on the website domain you expected!!
    - Double check the URL
    - Are there any weird characters, symbols?
    - Verify that you are on the correct domain before entering your login credentials
- Before typing in any personal data e.g. username and password, ensure that you have a ***secure*** connection between your computer and the shopping website.
    - You will know this because the website address at the top left of the browser window should begin with *http**s (with an "s")***

Fake AntiVirus

Fake antivirus software tricks you into purchasing and installing malicious software, which will pose as genuine-looking antivirus programs, but then grab your credit card information so they can "*fix*" your apparent virus problem.

They may show you a persistent pop-up window, warning that your machine is seriously infected with viruses, and offer to save you, by removing the viruses with their own software. But if you click anywhere in the pop-up window to close the message, the link instead goes to a fake website and your computer becomes infected with real malware.

The scammers may even call you by phone, and deceitfully inform you that your computer is showing "signs of viruses." They will then offer to "help" by directing you to a website to remove the viruses, but by following their instructions, you are basically granting full remote-control access of your computer to them!

You may also see browser messages for the following:

- Fake free security tools
- Fake security updates for applications and browsers
- Fake free computer performance tools

The good news is that most of these fake antivirus programs are *usually* non-destructive, meaning your files are not at risk of being destroyed by the malware.

- Instead they will keep pushing you into paying money to fix the made-up virus problem

Fake Antivirus Mitigation

Never respond to these fake antivirus alerts!

Because your company manages your antivirus software for you while at work, if you ever receive a suspicious message about viruses on your system, **please contact your IT support team or IT Security immediately.**

If you see these types of pop-ups at home, treat them with a high level of suspicion, and have your machine scanned for malware (or wiped and rebuilt from scratch if you wish to be prudent).

Banking Trojan

A banking trojan will secretly infect your computer or mobile phone, using some of the methods outlined earlier, and then hide and patiently wait for you to visit a financial website. Once it detects you have visited a financial institution's website, it springs into action, and injects extra fields into the login page - which ask for your personal details such as Social Security number and credit card information. It will also record your username/password, so that the hackers can later log in as you and steal your funds.

- Banking trojans can infect your system via malicious websites you may visit, or files you may download
- There are now many malicious ***Android*** banking trojan apps that pretend to be benign popular apps in the Google Play store (discussed in the Smartphone Security section below)

Banking Trojan Mitigation

- Review the banking login page itself to confirm it is the legitimate banking website:
    - If a financial website ever asks you on the login page for personal details besides your user name and password, **DO NOT LOG IN!**
        - *If this happens, there is a good possibility your system has been infected with a banking trojan!*
    - Call your bank, or walk into the bank branch to confirm that they are not asking for this information (which is extremely unlikely anyway)
    - Set up 2-Factor Authentication using an authentication app (as explained in the 2FA section below)
- You should ideally only have one browser window and tab open when logging into your banking website
- Ensure you have a secure connection to the banking website
    - The website address in the browser address bar should begin with http***s***
    - *This only ensures that your web connection is encrypted, not that the website itself is safe*

Mac Security

Today Apple Macs are *generally* safer to use than Windows systems

- This is because Apple controls their own operating system and hardware
- They are **very privacy-focused** as a company
- They keep a tight security lid on all new app submissions into their App Store
- Because of their smaller market share, there is less malware written for the Mac platform than for Windows
    - However, this is changing rapidly as more people buy Apple products (remember, hackers have no loyalty to Apple or Microsoft: they want your money!)
    - In the App Store there are ***some*** adware, spyware, and fake versions of software
    - Most Mac malware will also come from social engineering, e.g. fake software, fake browser updates, fake antivirus, fake security tools
        - E.g. *Fake* Adobe Flash Players for Mac desktops are VERY common! (Keep in mind Flash doesn't run on *iPhone/iPad anymore.*)
- There have recently been a few instances of MacOS cryptomining software
- Because Macs have **third-party apps** like QuickTime, and browsers and extensions, they can be used as a way to break into Macs, just like with Windows systems

Note: Many sophisticated Mac malware programs are highly targeted to specific individuals or organizations (for their secrets, or access to sensitive data, as opposed to money).

Mac Security Mitigation

Do not get comfortable with a false sense of Mac security!

The same secure behaviors you should exhibit on a Windows system are needed on a Mac, because most of the attacks outlined in this document apply to ***both*** Macs and Windows.

Keep your Mac operating system and all third-party software up to date with the latest patches:

- Open the 🍎 menu on the top left of your desktop, go to **About This Mac,** then **Software Update.** Then choose **Advanced,** and make sure **EVERY option is checked with a tick mark** to check for updates automatically from the App Store
- If you didn't download an app from the App Store, check with the software maker of the app for updates either on their own website, or via the specific settings of that particular application
  - Uninstall/disable your standalone Flash Player
  - Uninstall/disable Java from your system
  - The iTunes store is ***not*** a good place to buy any **security tools**:
    - Instead download antivirus software from a reputable company website yourself
    - **Sophos** and **Comodo** are both free antivirus for the Mac
    - **Cylance Smart Antivirus** is also great because it has machine learning built in, and can work effectively offline without any connection to the Internet

It is also good to use an "anti-malware" program alongside an antivirus program:

- **MalwareBytes** is great for catching adware, spyware and other such bad programs that antivirus programs might overlook
- It can run alongside antivirus programs such as Symantec, Sophos, McAfee etc.

At home, turn on File Encryption using FileVault on the Mac (at work, please work with your IT department if you travel with your work laptop and want to secure your business data). The latest Apple T2 CPU chips will also encrypt all your data by default now.

Apple's Safari is a good browser to use for privacy:

- It will block third-party cookies by default
- It also blocks browser fingerprinting now
- The latest MacOS has a full password manager built into Safari ☺
  - It will even warn you if you're re-using the same passwords across websites

Objective See is a fantastic website with many free security tools for the Mac:

- https://objective-see.com/products.html
  - **BlockBlock** will alert you anytime a program is installed to remain *persistent* on your system
    - Most benign programs install themselves to remain persistent, but so do evil programs, so it's important to keep an eye on which programs are trying to hang out long term
  - **Lulu** is a free firewall for the macOS
  - **KnockKnock** will scan your system for any programs that are installed persistently
  - **MicroSnitch** is a FANTASTIC tool that alerts you whenever you webcam, or microphone are activated

- **Do Not Disturb** is a great app that you can install when traveling for business, and will notify you on your phone if someone opens your laptop lid while you're not around

Little Snitch is a fantastic commercial personal firewall for the Mac:

https://www.obdev.at/products/littlesnitch/index.html

Smartphones & Mobile Apps

Our smartphones, such as the Apple iPhone and the various flavors of Google Android, are extremely intimate devices that allow you to view movies, browse, do online banking, take pictures and videos etc. So always keep in mind that they are essentially **mini-computers**!

And because they are so popular with all of us, they are major targets for hackers looking to steal our private data and money.

APPLE iOS

If you have an iPhone today, you are, IN GENERAL, more secure than on an Android. This is because:

- As mentioned before, Apple controls all of its own hardware and software
- Apple centrally notifies and pushes all iOS/app updates to all iPhones
  - These devices upgrade as soon as the latest versions come out
  - As a result, iPhone users are generally up to date
    - This website shows the most up-to-date install data for iOS products:
      - https://data.apteligent.com/ios/
- Apple has a closed app development environment, so it's harder for anyone to create an app for the iPhone
  - Apple has a very strict vetting process around the apps in their App Store
- Unless you "*jailbreak"* your phone, you cannot install apps from anywhere other than the official iTunes App Store
  - "Jailbreaking" is the term used to describe removing any restrictions Apple has placed on your iPhone, so you can essentially run any program you want
- **There is hardly any malware targeting the iPhone!**
  - Any sophisticated malware is basically nation state malware, which is significant because this means you're a highly prized target for another country!
  - There are however a few "Spyware apps" for monitoring kids etc. in the App Store (they are technically legal, but you need physical access to the phone to run them)
- The iOS permissions are more restrictive, and also easier for you to understand:
  - The app will also ask for permissions as it needs the permission in real time, which means you will have a better understanding of why it's asking

ANDROID

Android phones have incredible functionality, customization, and a more open development platform and App Store than iPhones, which offers us many benefits. But as a result, they also have some insecurities of which you must be aware:

- Google has little control over pushing software updates to ***non-Google*** devices ☹
  - So Google leaves it to third-party phone manufacturers to push Android updates to their own customers
  - Some phone manufacturers e.g. Samsung are now following Google's lead, and sending monthly updates to their phones

        - But many others either deliver them later or don't even bother at all!
    - Android users can download and install an app from *either* the Google Play App Store, or from any third-party Android app stores
        - **These third-party app stores have very little security checks if at all!**
        - They are many times open for anyone to upload any app of their choosing
        - A recent ThreatPost article states that the Google Play Store is 9x Safer Than Third-Party App Stores
            - https://threatpost.com/threatlist-google-play-nine-times-safer-than-third-party-app-stores/138964/

And most importantly:

99% of all mobile malware targets Google's Android OS!
- Which has caused 1% of all Android phones to have malware installed on them

50% of Android devices do not update to the latest operating system!
50% of Android users do not update their installed *apps to the latest versions*!

MALICIOUS ANDROID APPS

There can be thousands of malicious apps in the Google Play Store at any one time.

Malicious hackers often create copycat fake versions of popular legitimate apps:
- E.g. wallpaper/gaming/free games/productivity apps
    - These fake apps usually do what they advertise they will do, but once installed, will ask you for a bunch of excessive permissions, and then secretly download **far more evil malware code** to your phone!

Common things Android malware can do if downloaded:
- Ask for SMS permissions so that it can register you for paid services
- Send SMS messages to premium rate international numbers
- Spy on your calls and texts
- Steal your personal and sensitive data
- Steal your passwords
- Steal your banking 2-Factor Authentication SMS codes

Smartphone and Mobile Apps Mitigation

Use an Apple iPhone if possible
- They are much more secure in general
    - Apple's iOS will remind you constantly if there are any iOS updates
    - Remember to ensure you have turned on **"auto update"** for all apps and operating systems in your settings

If you use an Android, if possible, use a Google Nexus or Pixel
- The Pixel's Titan M chip introduces a lot of good security into the phone as well
- **If your phone manufacturer permits, upgrade to the latest Android operating system:**
    - It will make sure to activate Google's **"Play Protect"** feature, which will protect you by using Google Safe Browsing when you install apps and visit websites
    - Android now also force phone manufacturers to push regular security patches to your phones! **This is very important!**
    - Obviously, at your work, please securely manage the phone issued to you by your IT department, and follow all the recommendations in this document and training videos

Download apps only from trusted App stores/marketplaces
Install a security app on your Android for added protection
    - Some respected security apps include **Bit Defender**, **Avast**, **McAfee**, and **Sophos**. It's best to purchase a commercial version directly from the manufacturer, as there are many

fake antivirus apps in the Google Play Store that may trick you into installing them instead ☹

Be extremely careful to notice where your apps are being downloaded from Google Play

- **<u>This is especially true for Android devices!</u>**
- Always review the <u>app's permissions</u>, and notice any suspicious requests after you've installed the app
- *Never blindly grant permission to apps*
- Always vet the developer of any apps you download:
  - Vet the developer as if you were vetting a seller on eBay
    - What other apps have they created?
    - How many apps?
    - When did they start developing apps?
    - How many reviews does each app have?
    - What do the reviews say?
      - Note that hackers sometimes drown out bad reviews with their own glowing positive ones
- NOTE: Google is starting to remove any apps from Google Play that request permission to access your call logs and SMS text messages (and have not been previously vetted by Google).
-

As a precaution, turn on **iPhone iCloud** and **Google Cloud** backups of your important personal data. Trust me, you will thank us later!

- You can do this in the settings for either phone:
  - Here is a link that illustrates how to do it on an Android: https://www.wikihow.tech/Back-Up-an-Android-Phone-on-the-Google-Cloud
  - Here are two links that explain how to back up an iPhone to iCloud: https://support.apple.com/en-us/HT203977 https://support.apple.com/kb/PH12520

*IMPORTANT: Be very careful **<u>NOT</u>** to back up your sensitive company data to the cloud without their explicit permission and guidance! Please work with your IT department and refer to your official backup policies to make sure you are following their guidelines when it comes to your company's data.*

Also, be careful **not to save your company's confidential data** on any mobile device (business or personal), whenever possible.

- Again, follow your company's policies with regards to use and retention of sensitive data on mobile devices
- And 100% make sure your mobile device is password/PIN-protected!

Never leave your mobile device unattended, or in the hands of someone untrustworthy.

- It only takes a few seconds to view sensitive data on the device, or install a spying app
- **Notify your IT Security team immediately after you become aware of your mobile device being <u>lost</u> or <u>stolen</u>!**

- Never "jailbreak" your iPhone – doing so may allow you to download apps outside of the iTunes App Store, but you'll never know for certain which apps are safe to download from untrusted app stores (which are frankly rare anyway)!

<u>Signs you may have malware on your mobile device:</u>

- Slow Internet speeds
- Spikes in your data usage
- Large phone bill due to a new app that's using a lot of data
- Sending lots of premium SMS texts
- Your battery drains very quickly all of a sudden
- Phone connections frequently drop

At home, if you feel you have downloaded a malicious app, it is best that you wipe the phone via a **full factory reset**, and then restore your phone from a previous backup. (You have frequently backed up your phone right?! ☺)

At work, please contact your IT or Security department immediately and they will guide you on next steps.

FindMyiPhone & PIN Security

We cannot stress enough how important **PIN/password** protecting your phones and setting a **"Find My Phone"** feature is if you own a smartphone!

This literally takes a minute to set up.

PIN/PASSWORD

Setting a **PIN or password** on the phone helps in two ways:

- Prevents anyone from accessing the data on your phone in case it is lost or stolen
- It makes the phone encrypt/scramble all of your data (using your PIN/password) while the phone is locked
    - Until the correct PIN is entered into the phone, the data remains scrambled and unreadable ☺

iPhone defaults to a 6-character PIN but we strongly suggest you go into the settings and make it **8 characters!**

- While you're in the password settings, also set an auto-lockout time of **5 minutes or less**!

On a related note, don't use the **Swipe** feature to log into Android phones:

- It's very insecure because most people use predictable patterns (top to bottom, left to right and usually resembling letters e.g. Z, T
- It is also easier for an attacker to physically look over your shoulder when you swipe your PIN

FINDMYIPHONE

FindMyiPhone is awesome!

- Using GPS technology, you can:
    - Instantly see your phone's whereabouts, and communicate with it via a map
    - Send a personal message to the phone's screen
    - Lock the phone remotely
    - Wipe all your data on the phone in a few seconds
- iPhone has a **"Find My iPhone"** feature that can be set up through your iCloud account:
    - https://support.apple.com/en-us/HT205362

FINDMYDEVICE

This is the Android version, available here:

https://support.google.com/android/answer/6160491?hl=en

- Note: It is automatically turned on if you've added a Google account to your Android device

- Also, Android users can install an app called **"Where's My Droid"** for similar features and some really cool extra additions as well:
  - https://play.google.com/store/apps/details?id=com.alienmanfc6.wheresmyandroid&hl=enUS
  - https://wheresmydroid.com/

BLUETOOTH

If you're **not** using Bluetooth on your mobile device, the Bluetooth service should be *turned off!*

- But if Bluetooth is required, ensure that the device's ***"discoverability"*** is set to ***"hidden***" so that it cannot be scanned by a nearby Bluetooth device
- When using device **"pairing,"** ensure that all devices are set to "**Unauthorized**"
  - This will enforce authorization for each connection request

Password Management

Stop re-using passwords!

It's the leading cause of how people's accounts are hijacked!

Password strength depends on how many guesses a hacker would need to guess it correctly.
So to make your password stronger, you need to maximize these three elements of your password:

1. Make it **long**
2. Make it **complex**
3. Make it **random**

By **complex** we mean it contains special characters, numbers, capital letters etc.
By **random,** we mean it isn't easily predictable – for instance it shouldn't contain whole words or names.
The length of your password is exponentially more important than how many special characters and numbers you use!
So when choosing a password, it is ***more*** important to use a **LONG passphrase**, than a **short complex** password.
Literally adding ONE extra character makes it EXPONENTIALLY harder to crack!
We recommend having passwords of **16 characters** or more, especially for your sensitive accounts!

The best password to use is a LONG passphrase:

- First, think of a long catch phrase or chorus in a song you know:
  - e.g. **"Say Hello to My Little Friend"**
- Add a few special characters and numbers:
  - **"5ay H3llo To My L1ttle Fr13nd"**
  - This is your new *base* passphrase! Great!
- Next, for each *sensitive* account, vary your password slightly using **a few extra characters** that only you know and will remember:
  - e.g. "GL" for Gmail

- Your new long passphrase is: "**5ay H3llo To My L1ttle GL Fr13nd**"

VERY IMPORTANT NOTE: We strongly advise you to, ***if possible***, remember any passphrases for **email, and financial institution** websites in your own head!
These may only be half a dozen websites, so half a dozen variations of the base passphrase.
And for all the rest of the hundreds of website passwords one has to manage, we recommend you use a **password manager**…

==========

If you cannot remember your email and financial passphrases, then by all means store them in the password manager as well, but if you can do so, try to memorize only the **most sensitive ones**

==========

PASSWORD MANAGERS

Password managers capture your credentials, and then store them in an encrypted vault.

- The password manager will also offer to generate random passwords for each new site you log into:
  - For any new site logins, make sure to configure the password manager settings to only suggest 16-character passwords using lower and uppercase letters, numbers and symbols for all your auto-generated passwords
    - (Remember: these passwords do not need to be memorized)
  - Then you choose a master password so only YOU can access the vault
    - As long as you remember only the vault's master password, you can store hundreds of passwords in the vault! ☺

Note: Password managers are also wonderful, because they will *only* auto-fill your password into the login page *WHEN* they detect that the website is legitimate, and not a phishing page ☺
So if they do not auto-fill it may be a sign that you are on a malicious page

.

Setting up a password manager + setting up 2-Factor Authentication + setting a strong master password to encrypt your vault is the GOLDEN TICKET! ☺

You can choose either a **cloud** password manager, or a **local** password manager.
- What this means is simply that the manager will either store your password vault in the Internet cloud, or locally on your machine
- The benefit of the cloud is that your passwords can be synced across all your devices
  - Some password managers will also check your passwords, and flag any that have been reused in the past on other sites
- The benefit of local password managers are that your passwords never leave your system. This could be good if you are paranoid that you are a high-value target e.g. you work for a government
- Some reputable password managers include**, , 1Password** (my most recommended) **DashLane, KeePass** (and **Bitwarden** for a free alternative)

On a separate note, never save your passwords in your browser, UNLESS your browser has a built-in full-blown password manager:
- **The latest version of Apple Safari and Google Chrome now have free built-in managers**

- Your password will be stored in either Apple's or Google's cloud-based password vaults, and can be synced across devices

Some additional resources available to you:

https://www.wired.com/story/best-password-managers/
https://howsecureismypassword.net/

- This site will inform you how long it might take a hacker to crack your chosen password

https://haveibeenpwned.com/
https://haveibeenpwned.com/passwords

- This site holds a database of 500 billion email addresses and passwords that were stolen in recent breaches, and subsequently dumped on the Internet. Please check to see if your **email address**, or any of your **passwords**, have come up in any recent breaches, and don't forget to also create a **"Notify Me"** alert on the website for any future breaches that may contain your credentials! Finally, keep in mind that HaveIBeenPwned integrates directly into a good password manager called 1Password. The benefit of this is that if you use 1Password as your password manager, the service will automatically check all of your passwords against its database, and will warn you if any have been previously compromised on the Internet.

- *Recently, a HUGE 773 Million record database of username/passwords was found by @Troy-Hunt, the creator of HaveIBeenPowned Please check to see if your usernames/passwords are in that cache (they likely are) and stop using them for any websites that are important to you*

https://monitor.firefox.com/

- Firefox Monitor offers a service similar to Have I Been Powned, and will also alert your Firefox browser when you visit a website that has been part of a data breach in the past, by showing you a special icon in the address bar.

2-Factor Authentication (2FA)

TAKE NOTE! THIS IS AN EXTREMELY IMPORTANT TAKEAWAY FROM THIS TRAINING SERIES

Because passwords are constantly stolen, password security requires "defense-in-depth."

2FA essentially prevents people from hijacking your account!

If you want to keep using weak passwords (or the same password across sites) at least use 2FA!

You could even set all your passwords to "fluffybunny" and possibly be OK, because by setting up a 2nd factor, hackers would have to **steal your phone** AND figure out your **phone PIN** in order to access the **AUTHENTICATION APP** that generates your unique logon codes!

- Trust us when we say hackers HATE 2FA ☺

TOKEN-based 2FA > **SMS-based 2FA**

- Obviously, any kind of 2FA is better than just a username and password, but whenever possible, choose a "token-based" authentication app for your 2FA code (as opposed to SMS text)

    - SMS text codes can be intercepted, so cannot be relied upon for strong security
- Use Google Authenticator, or Authy for 2FA token-based app solutions
- This website will show you which sites have 2FA already set up for you to use:
    - https://twofactorauth.org/

If you are not sure if a particular site offers 2FA authentication, do a Google search for **"2FA and X website"** for instructions on how to set it up.

Here is a terrific website that shows you how to turn it on with many popular website

- https://www.turnon2fa.com/tutorials/

YUBIKEY AND SECURITY KEYS

Physical security keys such as the **YubiKey** and Google's **Titan** are considered the ***strongest*** of all two-factor authentication methods. They allow you to securely access websites such as Google, Facebook, Dropbox, Salesforce, GitHub, Stripe, and Twitter, and they also work tightly with password managers like **1Password**, **Dashlane** and **Keepass**.

To explain it simply, these keys are physical hardware, and they work by offering a one-time password (similar to what an SMS text or authentication app would do) that changes every 30 seconds. All you have to do, once set up, is simply plug the security key into your system and push a button on the physical key, which **generates a password that is sent to the website through an encrypted tunnel**!

These keys are *especially* useful if you're an activist, journalist, or other potential target of attacks, because *even if your weak password is stolen, the bad guys cannot get into your account without your* ***physical key!***

Tip: Another great thing about security keys is that if you try and log into a phishing website, the security key will not supply the One-Time Password, as it will know immediately the website is a scam!

PASSKEYS

FIDO2 is a new technology that is being welcomed by the major tech companies like Microsoft, Mozilla, Google, Apple etc., and to put it simply, what it does is **allow you to log into a website or mobile app with your *face ID, fingerprint, or security key*, RATHER than typing in password**

You may have already **noticed some banking apps logging you in this way**, and you will likely see this very soon across most popular websites..

Apple, Google and Microsoft announced game-changing commitments to support the FIDO2 password-less sign-in standard. And this year, all of the major browsers, platforms and operating systems – Apple, Windows, Android. iOS, macOS, Chrome, Firefox, Safari, Edge – will support FIDO2.

How does FIDO2 work?

Let's say you want to log in to a website or app that offers FIDO2 authentication. Instead of using a password, your smartphone will serve as your identity authenticator, by storing a passkey credential created using military-grade public/private key cryptography.

For each website or app, a unique passkey pair is generated. Stored in a secure device enclave and synced to the cloud, the private key never leaves the local device and can't be stolen. Meanwhile, the public key is sent to the online service and linked to the user's account. To log in, you'll receive a prompt from the website or app, to unlock your phone via biometrics or passcode. By doing so, your phone will sign a specific challenge with your private key, thereby authenticating you and your device to the service.

And if you lose your phone? Your passkeys are always securely backed up into the cloud, and should sync to any new device you own.

Using robust public-key cryptography, FIDO2 is uber-secure and phishing-resistant. The passkey process is end-to-end encrypted, so hackers cannot intercept them. Because the private passkey will never leave the associated device, a hacker can never masquerade as you.

On top of that, it's interoperable. Even if you're logging in with an iPhone, a Windows laptop, and a Chrome browser, FIDO2 will use Bluetooth to seamlessly communicate between different devices, and ultimately reduce any friction in the authentication process.

By eliminating passwords altogether, there is no need to reset or remember any passwords, and nothing to steal. Moreover, a passkey isn't sent unless the website or app is 'real', meaning fraudsters can't set up fake sites and use social engineering to steal credentials. As a result, credential stuffing, password guessing and phishing also become a thing of the past.

Furthermore, FIDO2 is both operating system and platform-agnostic, so there's no need to install extra apps, thus making it easier for mass adoption. Given that the three biggest tech giants are behind the standard, there's a good chance it'll be ubiquitous in the near future.

Everyone is tired of managing 100000s of passwords, for obvious reasons, so kudos to FIDO2 for making this happen securely.
Another cool thing about FIDO is that **it won't allow you to log into a fake phishing site.** It will ONLY present your credentials to the real website e.g. Amazon, and not a fake one like Amaz0n.

Google and many big online companies have already started to offer Passkets to their consumers. So whenever you are given the opportunity, I 1000% urge you to set one up. YOur login security will increase by 10x

Here is a link explaining Google Passkeys, and how to set one up for yourself in your Google account

https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password/

Expect many more tech companies to roll out Passkeys very soon.

A password-less Internet is definitely where the future is heading… ☺

SIM SWAP SCAM

Essentially, this attack is where hackers take over your mobile identity, by stealing your phone number!

SIM cards are small chips inserted inside a mobile device that authenticate the phone to the mobile network. They contain all your personalized settings, so by switching your SIM card into a new phone, you can easily take your settings, content and services/phone number with you.

The scammers take advantage of the fact that a **phone number** is used to authenticate people (similar to a password) and provide access to most services and accounts today.

So all a nefarious person has to do is impersonate you to your mobile phone carrier, and convince your mobile carrier to issue a replacement SIM encoded with your phone number to them. They can do this by:

- Calling into customer support
- Walking into a phone store and socially engineering/bribing a mobile sales rep to make the swap
- Working with mobile store employees who knowingly abuse their access to customer data and the mobile company's network

Now they will start receiving your calls and messages, and 2FA codes!

The best way to help prevent a SIM Swap attack, is to call your mobile carrier and **add a security PIN** to your account. Most major wireless carriers will let you add a PIN that needs to be provided over the phone or in person at a store before account changes can be made.
Note: If someone has illegal access to the customer database (for instance via a corrupt store employee) they can bypass the PIN.

Also make sure you always use an authentication-based 2FA app for logging into sensitive websites (as opposed to receiving 2FS SMS text codes).

You may also consider setting up a **Google Voice phone number that is tied to your Google account**, which forwards all calls/messages/2FA codes your own mobile number. You can tie your Google Voice phone number to any sensitive website account you have (in your profile settings). What makes Google Voice different is that Google Voice numbers can only be stolen if your Google password is hacked as well! Also, there is no customer service person who can be socially engineered to make a SIM swap.

Browser Security

One of the biggest leaks of privacy is via your browser and the websites you browse to – through the use of tracking cookies, browser fingerprinting etc.

As such your browser should be one of the most scrutinized applications on your system!

And so the #1 rule when browsing the Internet is to make sure that your browser is up-to-date!

JAVASCRIPT

Most websites use "Javascript," which is web code that allows you to have a very immersive and interactive experience.

- **Javascript adds all sorts of cool features and effects to the pages you view**
- ***But a lot of Javascript loaded on webpages is mostly extra, and not really needed***
  - Many of these scripts are actually third-party ads, trackers, and browser fingerprinters
  - Those scripts extract data about your machine and browser that can uniquely identify you, and then send it over to ad companies so that they can profile you, for the purposes of serving you targeted ads

TRACKERS

Third-party tracking scripts hang out on popular websites, and follow you as you visit different websites, carefully recording your browsing habits and interests.

Think of them as *peeping toms on the Internet,* as if a bunch of people are shoulder surfing you as you walk from aisle to aisle in the supermarket!

Most of the websites you visit will include third-party advertising and tracking scripts, including those placed by Google and Facebook to track your online activities.

In fact, on average, 50% of the total time required to load the average website is spent loading third-party trackers, which severely SLOWS DOWN BROWSING!

COOKIES

First-Party Cookies

- Cookies are awesome, making your browsing experience very personalized to you
- Most websites you visit set a cookie called a *first-party cookie:*
    - And in most cases, it is for analytics/functionality only
    - This kind of cookie is normally very important, and without one, site functionality would be sort of broken

Third-Party Cookies

- On the other hand, *third-party cookies* are added by companies whose sites you *aren't* visiting, but who are tracking your online habits and interests anyway
- On many sites, simply visiting a popular page will inject cookies into your browser for **over 50 different** third-party domains!

BROWSER FINGERPRINTING

Fingerprinting is a much more sophisticated and aggressive way to track you than cookies (and harder to avoid).

Marketers LOVE browser fingerprinting!

- Fingerprinting is a very invasive process whereby websites will collect technical data freely supplied by your browser to produce a unique ID that is tied to your browser, and can track you across websites to build an advertising profile of you
    - And this is separate from third-party cookies, which can be easily deleted by you if you wish
- They fingerprint your browser by collecting data such as:
    - Fonts you use
    - Your screen resolution and color depth
    - Your time zone
    - Which browser plugins you use
    - Your language settings

So EVEN IF YOU DELETE YOUR COOKIE, you can still be tracked via these browser fingerprinting scripts!

ADOBE FLASH

Adobe Flash is a multimedia software platform used for producing awesome web sites, games and video players, as well as web, desktop, and mobile applications.

However, it's being replaced by HTML5 which is native to your browser, so you don't need an extra plugin for it!

AND unfortunately, it has a TON of security weaknesses in it, so much so that it was completely deprecated in 2020!

And it's for this reason, hackers LOVE Flash!

- For instance, a common attack is where you might see a **fake Adobe Flash update message** pop up in your browser, or have malicious Flash embedded in a Word doc you download from the Internet

Browser Security Mitigation

- **Blocking JavaScripts can solve many of your cybersecurity problems on the Internet!**
    - But remember, you cannot 100% disable JavaScripts on all sites! If you do, you won't be able to use half of the sites on the Internet

- **But you CAN block third-party tracking scripts, third-party advertisements, and malicious scripts**
  - IMPORTANT: Depending on how often you visit the website, you can temporarily or permanently block scripts for that particular website:
    - If the website functionality stops working, you can enable scripts for that website one script at a time, or allow all scripts to run together (the worst case scenario)
    - Please choose wisely ☺

- For blocking Javascripts:
  - **NoScript** for Firefox
  - **UMatrix** for Chrome
  - **JS Blocker** for Safari

- For blocking trackers: **Ghostery** or **Privacy Badger**:
  - Both use artificial intelligence to learn which websites appear to be tracking you whilst you browse the web
  - Both learn to block tiny *'pixel-sized invisible* trackers on websites
  - They can send a **"Do Not Track"** signal to websites you visit
    - If trackers ignore your wishes to not be tracked, the blockers will block them altogether
  - These blockers will also mess with tracker inquiries that could be used to identify you, **by overwriting the fingerprinting data with random data** before being transmitted back to the trackers ☺
  - Ghostery will also automatically block and unblock trackers if it feels the tracker is slowing down your browsing, so as to maximize your online speeds
    - *Please keep in mind that there are some occasions whereby blocking trackers may break the functionality of the website you are visiting. If so, you can temporarily or permanently disable the blocking for that specific site in Ghostery or Privacy Badger*
  - *To trackers and advertiser, it's as if you have 'vanished' from the Internet* ☺

- For blocking advertisements: **uBlock Origin/AdBlock Plus/Privacy Badger all work well**
  - For Apple's Safari browser**: Magic Lasso**
  - For iPhones: **1Blocker X**
  - For Android users: Google banned many ad blockers from its Google Play app store, so the easiest way to block ads is to install a privacy-focused web browser like **Brave** / **Firefox Focus / Cliqz / Ghostery**

- **Use "private browsing":**
  - When your privacy window is closed, all history, cookies, and cached data are deleted from your computer
  - All three major browsers have their own version of private browsing:
    - Chrome = **Incognito Mode**
    - Firefox = **Private Browsing**
    - Edge = **InPrivate Browsing**
  - NOTE: The "private" or "incognito" browsing mode is **NOT** 100% private:
    - It doesn't prevent websites (Facebook/Google/Amazon, advertisers or your ISP from still tracking you
    - Only Firefox has "Enhanced Tracking Protection" to remove tracking from pages visited when in Private Browsing

- **Reset your Advertising ID:**
  - Android and Apple phones use an *"Advertising ID*" to help *some* marketers track you
  - You can go into your settings and delete the Advertising ID periodically

- According to Apple:
  - Whenever you want to clear the data associated with your Advertising Identifier, you can simply reset it
  - To reset your Advertising Identifier on iOS, open “Settings,” tap “Privacy,” tap “Advertising,” and tap “Reset Advertising Identifier”
  - To reset your Advertising Identifier on macOS, open “System Preferences,” select “Security & Privacy,” open the “Privacy” tab, choose “Advertising,” and click the “Reset Advertising Identifier” button
- For Android please follow the guidelines here:
  - https://www.androidguys.com/tips-tools/how-to-disable-personalized-ads-on-android/

- **Opt out of interest-based advertising**
  - Tech companies including Google, Facebook, Twitter and Apple offer instructions on opting out of receiving ads based on your interests (see the following section on Internet Data Privacy)

Keep in mind that all of the above steps won’t stop advertisers showing you **ALL** ads, but it will clear out any profile they may have gathered about you thus far, so you can start with a fresh profile and no targeted ads.

- **Remove Flash!**
  - The latest versions of Chrome, Safari, Firefox and Edge block Flash by default!
    - Go into your browser plugin settings and enable **“Click to Play”** for Flash!
  - **For help removing Flash from your home system, please refer to these helpful guides on the Internet. It literally takes a minute of your time:**
    - **ON WINDOWS:**
      - **https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-windows.html**
    - **ON MAC**
      - **https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-macos.html**

- **Use DuckDuckGo as your search engine for private searches**
  - They promise to never store your personal information, or track you for the purposes of serving ads
  - Here is a fantastic article by the CEO of DuckDuckGo explaining why they do not track your searches, and how their business model doesn’t make you a product:
  - https://www.quora.com/What-is-the-revenue-generation-model-for-DuckDuckGo/answer/Gabriel-Weinberg

- **Use VPNs for privacy**

- Add the **HTTP Everywhere** browser extension

- **Use the PanoptiClick website:**
  - Tells you if your browser is blocking tracking ads and if it has a unique fingerprint on the Internet

- **Verify the default cookie settings is to block third-party cookies**
  - Please keep in mind that there may be some occasions where blocking third-party cookies *may* break the functionality of the website you are visiting. If so, you can temporarily or permanently disable the blocking for that specific site in the browser settings

- **Set your browser to automatically clear your browsing data when you close it**

If you wish to save the time from installing all these plugins/add-ons then simply use either the **Brave / Ghostery / Cliqz Browser!** (There are both desktop and mobile version)s of each

Note: Here is a great article that guides you through your privacy settings on each major browser:
https://www.wired.com/story/how-to-lock-down-websites-permissions-access-webcam/

- **When browsing, always be aware of which websites you are visiting:**
  - Look for letters in the address URL that look like another letter or number, or additional letters or numbers
    - e.g. “Amazon.com” vs “Amaz0n.com” vs “Amazoon.com”

- **And keep in mind that up to 50% of malicious phishing sites are hosted on benign sites that have HTTPS secure connections!**
  - You will see a green padlock sign in the address bar, even though the site is hacked!
  - Hackers do this because they know you will have a false sense of security when visiting, and when you see “HTTPS” in the browser address bar
  - Having said that, if you are *either logging into, or purchasing something* from a website, if you **don't** see “HTTPS” in the address URL, **do not log in, and do not buy anything!**
    - This means you don’t have a secure connection, so someone can intercept your credentials or credit card information on the Internet!

WHICH BROWSER TO USE

Firefox

- **Great for privacy!!**
- Firefox does not make money from tracking users or selling targeted ads
- **Caveat: You must install ad and tracker blocker add-ons though!**
- Firefox contains **built-in phishing and malware Protection**
  - Works by checking the sites that you visit against blacklists of reported malicious sites
- **The latest Firefox browser version blocks:**
  - Browser fingerprinting
  - Tracking cookies
  - Cross-Site Tracking scripts
  - Cryptominers
- The browser also:
  - Speeds up webpage loading times, by blocking the slow loading trackers
  - Has DuckDuckGo search engine as an option in the Firefox Settings

Brave Browser

- Brave is built on the same platform as Chrome
  - **But it is completely focused on privacy!!**
- Brave is a **very fast** browser because it blocks so many trackers and extra “bloat” from loading in your browser
- Brave’s privacy is all about not collecting sensitive data in the first place!
  - They are not in the business of selling your data
- *Brave is basically ready out-of-the-box to be used for blocking ads and trackers*
- Brave browser includes the “Brave Shield” which does the following:
  - Blocks ads
  - Blocks tracking requests

- Blocks known phishing or malware sites
- Forces your browser to use a secure SSL web connection whenever possible
- Blocks browser fingerprinting
- Has DuckDuckGo as a search engine by default
- Has "Tor in the Tab" which prevents websites from tracking your location

Ghostery and Cliqz Privacy Browsers

- Ghostery and Cliqz also offers great privacy-focused browsers!
- Either of them is very much worth checking out
  - https://www.ghostery.com/
  - https://cliqz.com/en/

Chrome

Excellent in security, weak in privacy

- Chrome does a good job trying to keep you informed of malicious websites and content
- The upcoming version of Chrome will even warn you if you accidently navigate to a lookalike website e.g. g00gle instead of google
- Note: Google is an ADVERTISING company, so Chrome is not PRIVACY friendly
- *Chrome essentially collects your browsing history, as well as things you search for or do*
- Chrome **extensions** are the browser's Achilles heel!
  - Google is seriously vetting its 180,000 extensions in the Chrome Web Store, and will **only** allow you to install extensions from the Google Play Store, especially the extensions that ask you for extra permissions once you've installed them
  - *So be very careful about which extensions you download!*
  - Do your research, and vet them just as you would if you were to purchase something from eBay!
  - **It's best to keep extensions to a bare minimum on your browser**
- Safe Browsing handles the security in all of Google's major products:
  - *Gmail*
  - *Android*
  - *Google Ads*
  - *Google Search*

So when you visit a website, or choose a **Google Play app**, Safe Browsing will check for malicious behavior and warn you with a big, red warning if it:

- Hosts malware
- Tries to install unwanted software
- Tries to modify your search engine
- Accesses phishing sites

Windows Defender Browser Protection

This plugin brings Edge's phishing protection to Chrome as an extra defense-in-depth:

https://chrome.google.com/webstore/detail/windows-defender-browser/bkbeeeffjjeopflfhgeknacdieedcoml

Tor Browser

Note: please do not use the Tor Browser at work. Only use the browser installed by your IT department.

If you want FULL privacy + anonymized web traffic at home:

- The browser already comes with pre-installed privacy add-ons etc.
  - Tor is way better than *Private Incognito* mode and **will actually stop tracking**!

        - It does this by isolating each website visited, so third-party trackers and ads can't follow you, and it automatically deletes all your cookies when you are finished browsing
    - And as long as you don't ***log in to*** any websites, the website won't know who you are, and therefore from which country or location you are visiting

Microsoft Edge

- MS Edge browser is a secure browser in general
- But it is not very strong on the privacy side of things
    - Although, they do have a **"Do Not Track"** feature on by default in IE10, which instructs websites not to track you (*websites don't always comply with this request by the way*)
- It has great defense-in-depth protection built in, such as the **Smartscreen filter**
    - It will tell you whether you're visiting a malicious website, by performing reputation checks on the website, and then displaying a bright red page if it is flagged
- Microsoft Edge extensions can be installed through the Windows Store, although they don't have many extensions in comparison to Chrome and Firefox
- For Edge, use: **uBlock Origin** + **AdBlock Plus** to block ads**,** and **Ghostery** as a tracker blocker
- Unfortunately, Edge does not have a good script blocker ☹
- Edge has decided to use Chrome's internal 'Chromium' engine in the future, so this will have privacy implications, as well as give Google control over most of the Web (as Chrome will be the most used browser by far).

Apple Safari

- It could be argued that Apple's best product is its actual commitment to privacy, as opposed to its premium laptops and phones
- Safari was the first browser to take privacy seriously and block third-party cookies by default
- The latest version of Safari will do the following by default:
    - Block browser fingerprinting
    - Block third-party cookies by default
    - Safari's **"Enhanced Intelligent Tracking Protection"** blocks Cross-Site Tracking
    - Limits the data that websites can extract from the browser
    - This will basically make your Mac browser look more like everyone else's on the Internet ☺
- **Block social media "Like" or "Share" buttons and comment widgets from tracking you without your permission:**
    - Facebook and Google can track your movements around the web via the embedded "Like" and "Share" buttons on web pages, or via the Facebook Pixel
        - **Facebook Pixel** is a tiny pixel, hidden to the naked eye, that is displayed on websites ***other*** than Facebook
        - It will tell Facebook where you have been outside of Facebook
        - So if you're logged into Facebook for instance, and you open another browser tab and visit a site (that has the Pixel or embedded "Share" and "Like" buttons), Facebook will be notified you were on that website!
        - **The good news is that the pixel can be blocked by Ghostery!**

Social Media Scams

Because of all our connections with friends and family, as well as our *ability to share new photos, links, comments and stories with them,* social networks are a very effective way of spreading evil malware.

And because there are over a billion people on social media websites, hackers and scammers go to where people congregate! It's paradise for the bad guys!

Thus, because of this inherent trust you have with your social media friends, hackers and scammers will use social engineering to trick you into viewing pictures and videos, and visiting links that will bring malware to your systems (because you are more inclined to click on something that has been "shared").

As a result, please make a habit of **only** following current news and events on ***reputable*** news sites, and avoid reading news on social networking sites such as Facebook, unless the article is from a reputable news source as well.

- **Stop, and pause, when a friend sends a message, or writes on your "wall" with a catchy subject line, to persuade you to click on the link, such as:**
  - **OMG!**
  - **WOW!**
  - **YOU MUST SEE THIS!**
  - **HEY, CHECK THIS OUT!**
    - This is especially important if it appears the content is about *something very sensational, contentious or provocative*

- **ALWAYS** receive your daily news from a reputable news source such as CNN, Fox, Reuters, BBC etc.

- **Be extremely careful which social media groups and profiles you follow**
  - Although Facebook/Instagram/Twitter are deleting millions of fake accounts on a daily basis, new ones are still created to share false or malicious content

- Be very suspicious if a message prompts you to update a program e.g. video codec, in order to view content

- Be very suspicious if a message asks you to grant a third-party app access to your profile

- Think twice before accepting friend requests from people you don't know
  - There are millions of bogus social media accounts created every day, with fake profile pictures, which are being used to social engineer people

False News

There is an information war going on right now on social media, with influence campaigns being conducted by many of our adversaries to change our public opinion about them, as well as change political discourse in our country!

False news spreads faster and is 70% more likely to be re-tweeted than real news![1]

The issue today is that most people get their news from Google and Facebook, and they follow news sources and groups that "tell you you're right." In other words, the news they read will be biased to lean towards their own political opinions, no matter what side of the political spectrum they are on (which

[1] http://science.sciencemag.org/content/359/6380/1146

pushes people into echo chambers and can even radicalize some of them). And because some people unfortunately cannot differentiate between what is fact and what is opinion in news articles, *the line between news and entertainment has recently been blurred.*

The other issue is *cognitive bias*, where once you've read something as news, it's difficult to discount it as false (even if it's proven to be false after the fact). And this is especially true when you already agree with the premise of the statement e.g. "Hillary Clinton isn't trustworthy," or "Donald Trump is self-serving." So as a society, we end up with a situation where ignoring outright lies becomes difficult.

Moreover**,** a new phenomenon started a decade ago, where social media enabled anyone to be a content creator. Many people can now amplify what they think about a topic, and grow a captive audience with little to no budget and no editorial oversight. That is a huge advance for us as a civilization, but what if the message is a lie, propaganda, or outright malicious?

Remember: social media is as good at bringing people together around the world, as it is at spreading paranoia, misinformation, conspiracy theories and propaganda via news articles and political advertising.

During the 2016 U.S. Presidential elections, it has been determined that millions of people followed **Russian trolls** on Twitter, Facebook, Instagram and Reddit and were duped into reading ***precision-targeted political advertising***. The trolls created accounts on every side of the ideological spectrum, and then would share inflammatory articles and misinformation posts to increase tensions among us, and widen the divide in American culture.

The aim of the Russian trolls was not to try to change your mind about a particular topic, but rather exploit divisions in order to break down our society into smaller, warring groups. They wanted us to start to question truth as it really is, and ultimately make democracy look weaker compared to autocracy.

So with the use of inflammatory hashtags, partisan conversations and offensive pictures, hundreds of thousands of social media users were tricked into spreading misinformation.

Why does this **affect cyber security specifically**? Well, because websites and social media accounts/groups that knowingly spread *falsehoods*, can just as easily **spread malicious code via posted files, messages, videos, and webpages**!

False News Mitigation

- Always do your research and be very wary about where and how you receive your news!
  - ➔ If possible, try to avoid getting your political news from social media!
- **Distrust anything you initially read, and be aware of false news related to trending current topics**
  - ➔ We all need to think more critically about our news, even if it aligns with our political views
- Facebook and Twitter now judge an account on its TRUSTWORTHINESS
  - If you share any content that Facebook's non-partisan fact checkers deem to be false, your account's trustworthiness will be demoted, and sharing future content will become more difficult for you
- Keep in mind Twitter accounts can be created and managed by an automated bot (they don't need to be verified by Twitter to be active), whereas Facebook and Instagram accounts need real human interaction be active
  - ➔ On Twitter, always check the URL and the USERNAME of the account:
    - Important: the account name, followers, tweets and posted images can all be fake
    - See if the account is "verified" with a blue tick mark next to the Twitter name
- Look for suspicious things like capital "i's" that look like "l's", or "O's" that look like "0's"
  - This indicates a scam account

Internet and Social Media Privacy

The Internet has recently been likened to “surveillance capitalism.” This may be a bit of a drastic and ominous assessment, but it is a fact that we are all being tracked on the Internet on a minute-by-minute basis, especially by many major tech companies.

Because their revenues and business model are based around presenting advertisements to us, it is in their interests to monitor our web traffic across the Internet, so that they can then monetize this data in the form of targeted advertising.

For instance, Google will create an **“**Advertisement Profile,” which may include the locations you visit, age, gender, career, interests, hobbies, relationship status, and income.

This profile may be gathered from:

- Search history
- App and extension usage
- YouTube history
- GPS location
- Gmail activity

Another issue is that many websites let you *“conveniently”* prove your identity by using your Facebook, Google, or Twitter credentials to log in:

- *But by doing this, you are allowing these tech companies to access, and monetize your profile and activity*
- So please, take the extra step and create a separate account on each site (using your password manager ☺)

Internet and Social Media Privacy Mitigation

We need what some people are referring to as a **“Data Detox”!**

Tune your privacy settings for Google, Facebook, Instagram, Twitter, Amazon, Apple, Microsoft, etc. (Each of these company’s products has a settings page where you can this.)

Facebook

- Review your Facebook privacy settings:
  - Check how others view your profile
  - Limit the audience on previous posts
  - Lock down the privacy on future posts

- Restrict your Facebook ad settings: https://www.facebook.com/settings/ads/

- Review the information Facebook has about you: https://www.facebook.com/settings?tab=your_facebook_information

- Manage your invites, uploaded contacts, call and text history: https://www.facebook.com/mobile/facebook/contacts/

- Review which apps/games/quizzes have access to your Facebook profile: https://www.facebook.com/settings?tab=applications

- Remove as many third-party websites, games or apps as possible that are connected to your FB account:
  - Check out their permissions
  - See what information you're sharing with them

- Set up good security and 2FA for your Facebook logins: https://www.facebook.-com/settings?tab=security

- Avoid doing any online quizzes/surveys on any social media websites

- Never browse to other websites when you have an open Facebook tab
  - Close your Facebook tab first (this prevents a lot of the snooping that Facebook does on your online activities)

Google

Check your Dashboard, Privacy Checkup, Activity and Ad Settings:

- **See and manage the data in your Google Account:** https://myaccount.google.com/u/1/dash-board
  - **For maximum privacy, scroll down to the "Your Activity Data" section, and set all the services to *"PAUSED"***

- **Review and adjust what data Google knows about you:** https://myaccount.google.com/u/1/privacycheckup/

- **Turn Off Ad Personalization:**
  - You can turn on/off Targeted Ad settings based on interests that Google thinks you like: https://adssettings.google.com/authenticated

- **Review/delete all your activity information Google has collected about you:** https://myactivi-ty.google.com/myactivity
  - To delete all your information from Google's major services: https://myactivity.google.com/delete-activity
    - Click on "**delete activity by,**" select "**all time**" and "**all products,**" click on sub-mit

- **And review more activity here:**
  - https://myactivity.google.com/more-activity

- **Download all your Google Data!**
  - https://takeout.google.com/settings/takeout?pli=1
  - NOTE: Many Google services on Android and iPhones store your GPS data, even when you have paused "Location History"!
    - **To ***actually*** turn off location tracking, go to *"Web & App Activity"*:** https://myaccount.google.com/activitycontrols/search
    - **Also visit this link delete your main location history here:**
    - https://www.google.com/locationhistory/delete

For stricter privacy controls, refrain from using the combination of:
Android phone + Chrome Browser app + Google Search app

This will greatly reduce the amount of data Google collects about you when on the Internet!

- According to recent research, it was discovered that an "idle Android phone sends 10x more data to Google than an iOS device sends to Apple"[2] in any given hour. And half of this communication was determined to be with advertising services
    - Also, an "an idle Android phone running Chrome sends back to Google **nearly 50 times** as many data requests per hour as an idle iPhone running Safari"
    - This data is transmitted to Google servers, and used for targeted advertising and building your user profile

Finally, do not *log into* your Google account *within* the Chrome browser, if you do not want your web, bookmark and search activities being synced to your Google account.

How to delete your Google account or a Google service

Here is a great article by Cliqz that explains how to delete your Google account altogether:

https://cliqz.com/en/magazine/how-to-delete-your-google-account-or-a-google-service

Twitter

Once logged into Twitter on the web:

1. Click your profile icon in the top right navigation bar
2. Select Settings and privacy from the drop-down menu
3. From the menu on the left, click Your Twitter data
4. Enter your password and click Confirm

Apple

Because Apple earns revenue from selling high-end phones and laptops, their public position is that they are, unlike Google and Facebook, not in the business of collecting and analyzing your data for the purposes of targeted ads, and that they take our privacy very seriously. To state it simply, Apple asserts that privacy is our **human right**!

Please be aware that Apple **does** collect user data. However, its policy is to collect as ***little*** user data as possible to make their products work. And when they do collect our data, they anonymize as much of it as they can. In fact, most of the data an iOS device sends back to Apple is scrambled using a technique called "Differential Privacy," which **adds random junk to your data before it reaches Apple,** so the company has no way of knowing that it came from your device.

Moreover, Apple stores most of your personal and sensitive data **locally** on your mobile device, and sends a small amount to its servers for targeted advertising.

Having said this, Apple has a privacy website, where you can review/download all the data Apple has about you: https://privacy.apple.com/

They also have a general website that addresses all your privacy questions: https://www.apple.com/privacy/

[2] https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/

Finally, please stop using Facebook/Gmail/Twitter as a sign-in service to other websites

And if you want to go super private, use an iPhone only, and do not use any apps owned by Facebook or Google!

Identity Theft

The Federal Trade Commission says it can take only 9 minutes to buy and use our stolen details on the underground market to **open credit cards and bank accounts, apply for mortgage loans etc.**

And because the Equifax hack involved 200 million credit profiles that included full names, Social Security numbers, all addresses, driver's license numbers etc. we should all consider our personal information to be somewhere on the dark web by now.

Another issue is that there are many websites on the Internet that will provide access to your credit report with only a simple search, even if the search includes typing in an incorrect Social Security number!

So because is quite easy to access someone's credit report these days, it is vital that you **FREEZE** your credit report!

Identity Theft Mitigation

- Contact all 4 main credit agencies noted below, and set up a free **credit freeze & fraud alert!**
    - **To place a credit freeze, you must contact each of the four credit bureaus individually to set up the freeze**
        - https://www.transunion.com/credit-freeze
        - https://www.experian.com/freeze/center.html
        - https://www.equifax.com/personal/credit-report-services/
        - https://www.innovis.com/personal/securityFreeze

- *It serves as **2-Factor Authentication** for your credit profile!*

- **Credit freezes and fraud alerts are FREE!**☺
    - Fraud alerts last for one year, but you can renew them each new year!
- Credit ***freeze*** or ***lock*** are used interchangeably, and offer similar protections
    - However, it's important to note that credit freeze promises to guard your credit accounts, and this is guaranteed by law! With a credit freeze you won't be targeted by ads
    - It takes five minutes to set up a freeze, and to unfreeze, you will use a 10-digit pin
    - On the other hand, a credit lock is an agreement for protection between you and the credit agency, and it is ***not legally covered by law***
        - Having said this, credit locks are easier to lock and unlock
    - A fraud alert is an extra precaution, so that no one can grant credit in your name, without first contacting you to obtain your approval
        - **To place a fraud alert, simply notify any one of the four credit bureaus, and they must automatically inform the other three of your choice for an alert**

Here is a fantastic article by Brian Krebs, a noted security researcher, explaining in more detail where to set up the freezes:

- https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Finally, credit monitoring services can be useful for notifying you "*when"* someone opens a new line of credit in your name. But this is **after the fact**. They won't prevent identity fraud from occurring in the first place the way a credit freeze does.

Keep in mind that a credit freeze will not save you from hackers who file a fraudulent tax return in your name, or use a stolen credit card to make payments.

NOTE: You can recover from most fraud incidents if you detect them within 24 hours, but after 72 hours the fraud will be hard to reverse (because it takes a significant effort to correct your reputation, credit rating and privacy).

The Federal Trade Commission also maintains a website to help you detect and recover from identity theft, by teaching you how to monitor your credit and look for early warning signs of identity theft:

- http://ftc.gov/bcp/consumer.shtm

They also have great fraud/scam alerts to which you can subscribe.

GDPR/CPRA

GDPR is EU regulation that states EU citizens have a right to know *what data about them is being collected, why, and for how long it is being stored. And CCPA/CPRA is a California law that is similar to GDPR in many ways*

Please note the following GDPR rules, both as a consumer, and as someone working for a company such that manages data for citizens of the EU:

- Only collect user data where there is a ***"lawful basis"*** to do so
- Data is only to be collected and saved for "***specific***, ***explicit***, **and** ***legitimate*** **purposes"**
- **Only collect data with the user's explicit consent:**
  - User needs to be told what is being collected
  - Why it is being collected
  - Who it has been shared with
  - This collection must be clearly documented, and consent can't be assumed, or buried in a bunch of terms and conditions
- **User data shall only be stored and processed for as long as it is required, and no more:**
  - So always consider what kind of data you're collecting
  - And whether that data even needs to be obtained in the first place
- **The user's data must be kept up to date and accurate**
- **Update your company's data collection processes so you can:**
  - Identify all data repositories
  - Classify which data is personal, and which data is not
  - Follow "privacy by design" principles, similar to what Apple does
  - Centrally control access to this data
  - Monitor how the data is being used
  - Anonymize or encrypt all personal data
  - **Ensure that data retention and recovery policies are very defined**
- **The user has the right to receive a copy of their data**
  - Or request that their personal data be deleted entirely, to be "forgotten."
    - *They can request that a company delete their data, stop sharing it and/or stop third-party firms from using it*

- **If you do have a data breach, it needs to be reported within 72 hours after you become aware of it:**
    - IMPORTANT: If you encrypt all customer data as well as the encryption keys, then you *might* not be obligated to notify
    - **So for GDPR data, make sure you ENCRYPT everything!**
        - Emails, data in your cloud repositories, data being sent online, hard drives, thumb drives etc.
    - Make sure you are properly trained in how to secure and protect the data
        - If you're unsure, please work with your IT or IT Security departments to receive this training
- **Failure to comply with GDPR can result in fines up to 4% of your company's global revenue**

Encryption

Before considering any encryption solutions, make sure you ***do not*** go outside of company policy and install unauthorized encryption software.

Now, having said that, encrypt as much company and personal data as you need, to make the data unreadable to prying eyes…☺

Some of the things you can do are:

- Store your company data in an encrypted file server at work
- Encrypt your full hard drive using **Bitlocker**, **Filevault** or **VeraCrypt**
    - (This also *prevents a thief from even starting your laptop without a passphrase!)*
- Encrypt your files using software such as **VeraCrypt, 7 Zip, Bitlocke**r and **PGP (or the free version GPG)**
- **Use a free program such as VeraCrypt, which encrypts an entire partition or storage device such as USB flash drive or hard drive.**
- Password protect your files using **WinZip**, **WinRAR** or **Apple Mac's Disk Utility**
- All web sites and traffic, slowly but surely, are becoming encrypted on the Internet:
- 75% of the web is now HTTPS encrypted! ☺
    - However, some websites are HTTPS ready, *but* won't serve you HTTPS encrypted pages by default
    - To help things along, install a plugin called **HTTPS Everywhere** into your browser
        - It forces these websites to serve you encryoted Secure Socket Layer (SSL) pages BY DEFAULT,
            - *(which means the traffic is scrambled/encrypted and unable to be read en route by anyone)*
        - **Brave** has this pre-installed in their browser
- Make sure to encrypt any emails that contain sensitive client/customer data, or personal data such as Social Security numbers
    - Your IT department at work may have an encryption solution already deployed for you
        - At home, you can install solutions such as **PGP** or **OpenPGP**
- At home, if you wish to use a free web-based email client, **Gmail** offers great **security** for the price. They do a very good job warning you about malicious emails that come into your inbox, as well as filtering out Spam and dangerous emails as well.
    - If you want security AND added privacy, we also strongly recommend **ProtonMail**
    - They use encryption software called GPG, which is similar to PGP, to encrypt all your emails, simply by you choosing an encryption/decryption password for your messages
    - **ProtonMail cannot read anything,** because the encryption happens in the browser on your computer, not their servers
    - Email recipients don't receive your actual email, but rather a *link from ProtonMail* to view that email

    - ProtonMail even allows you to set an expiration time on the message!
        - Note: Gmail also allows you to set similar privacy controls around specific emails you send
    - ProtonMail also does not keep a log of your IP address, so they cannot trace anything back to you!
    - **CryptText** is a new solution that states they are even more secure than ProtonMail
    - Another very well respected encrypted email solution is **Tutanota**
- Alternatively, you can type a secret message in a Word document, and then password protect/ encrypt the file itself! Then **send the protected file in an email** ☺
- Use ***DEFAULT*** end-to-end messaging solutions such as **Signal**, **WhatsApp** and **Apple's iMessage**
    - End-to-end means the contents of your message travel directly from you to the receiver, without being intercepted and read midway
        - The decryption key is stored *on your device* and anyone intercepting has no way to decrypt your messages
        - Signal is FANTASTIC. It is non-profit and open source, and offers the highest level of encryption architecture in a messaging app
        - Signal not only encrypts your messages, but only the message recipient can see who sent the message to them.
        - ***No-one can intercept and see who is communicating!***
    - **Do NOT send sensitive information via messaging apps** such as Snapchat, Telegram or Facebook Messenger
        - **They do NOT have end-to-end encryption set *BY DEFAULT***
        - **Instagram has no end-to-end encryption at all at the moment** ☹
        - Facebook Messenger only offers this encryption feature **if you turn on "Secret Conversations**.
    - Facebook intends to **integrate all 3 messaging platforms it owns: Instagram, WhatsApp and Facebook Messenger**.
    - Facebook will upgrade Instagram and Messenger encryption **to match WhatsApp** when they all merge, and not vice versa (by the way it never hurts to keep super secrets chat off Instagram and Messenger for now until this is resolved)
    - NOTE: For messaging someone, end-to-end encryption can sometimes be a better way to communicate personal secrets than via email!
        - *For work, please follow strict guidelines set forth by your IT and Security departments for communicating with customers and clients about sensitive matters*
- *Whenever traveling, use a VPN client to conduct business, and to secure your web traffic in open WiFi locations such as airports, hotels and coffee shops:*
    - You can use a VPN on your laptop, phone or tablet
        - All your web traffic will be encrypted before leaving your system, and will make your VPN provider be your "first hop" on the Internet
        - For this reason, you need to trust your VPN provider a lot!
        - Here is a good resource to pick between 150 different VPN clients: https://thatoneprivacysite.net/vpn-comparison-chart/
            - (They also have a good email security section)
    - To make it easy, we recommend **NordVPN**, **ProtonVPN**, **TunnelBear, Express VPN, and Perfect Privacy VPN**
        - VPNs will mask your IP address, and remove tracking cookies, which is great for privacy!
        - ProtonVPN and NordVPN also offer access to TOR for ultimate anonymized traffic
            - ***Note: if you want exceptional privacy and anonymity, you can connect to the TOR network AFTER you have established a VPN connection with your VPN client***
            - ***Its best to use a VPN service, such as NordVPN, that allows you to connect to Tor servers. Then use the 'Onion Browser' from Tor, once you have connected to the VPN network, to browse***
                - ***This is AMAZING privacy and anonymity!***

        - Use the **HTTPS Everywhere** plugin as well, to try and enforce that your HTTPS connection is end-to-end encrypted from your browser to the website you are visiting
        - TIP: To remain anonymous on Tor, never log into any web mail or social media accounts, so that your identity is never accidentally exposed
        - ***Please do not try these at work, this is strictly for anonymity whilst browsing at home***
    - VPNs have different tiers depending on subscriptions

Some additional resources:

- https://www.wired.com/story/securely-share-files-online/
- https://www.wired.com/story/smartphone-encryption-apps/

Business Travel

First and foremost, always ask your IT department to install any free or commercial software needed to work securely whilst traveling.

Now let's cover some very important points when it comes to traveling for business:

- Take heed of the previous section about encryption, and encrypt any sensitive data you have on your laptop with the help of your IT department
- Ensure your phone/tablet is password protected
    - Turn off all biometrics logins (authentication using parts of your body) when traveling, as customs officers in foreign countries may unlock your phone using your face or fingerprint
- Only work on company data using company-issued devices:
    - NEVER use personally owned devices for work
- When traveling, only carry what you need remotely to do your assigned work
    - As a rule, "don't bring what you don't need"
    - If you have to travel with stored data, make sure its encrypted!
    - Or keep it on an encrypted department file server back at work, or securely in the cloud
- When traveling, it is imperative that your laptop **is encrypted using special encryption software** installed by your IT department:
    - If you are uncertain, please ask your manager and/or IT for help
    - Tape a phone number to the bottom of the laptop and to the charging cord
    - If a good citizen discovers them, he or she can contact you to arrange for their safe return
- Always leave your laptop in the trunk of your vehicle, and never in plain sight on a seat
- Do not connect to a public Wi-Fi, unless you're using a VPN client:
    - **ESPECIALLY for company work, banking, or e-commerce websites**
- **Only connect to well-known Wi-Fi networks**
    - Always check the network names to make sure there are no extra characters or typos
        - Pro tip: Tether your laptop to your mobile phone's ***hotspot***:
        - This bypasses open WiFi connections, and instead uses your mobile cell service to connect to the Internet
    - Also switch off your Wi-Fi and Bluetooth connections when not in use
- **Turn off any biometric login features on your devices, so you can ONLY log into the device using a password or PIN**
- **Be alert at the airport:**
    - Always take your laptop as carry-on luggage
    - Keep an eagle eye on your laptop as it is security-screened:
        - Do not walk through X-ray *until* your items are next on the conveyor belt for X-ray

        - If you use your laptop at the airport, place it in front of you and/or use a cable lock:
            - Do not place it on the floor:
                - A thief might slide it their way
            - On a plane, store the laptop in your bag under the seat **in front of you:**
                - Avoid placing it in a plane's overhead storage area where it may be knocked around or damaged by heavier bags, or stolen
- **Staying overnight:**
    - When possible, try not to leave anything of value in your hotel room
    - If you leave your laptop in a hotel room, **always use the hotel room safe**
    - When you leave the room, leave your TV and lights on, close the curtains, and hang a "Do Not Disturb" sign to make it appear that you are in the room
    - Also, take care to close the latch and deadbolt your door *after* entry
    - Immediately contact your IT department if the device is missing, stolen or tampered with

IoT and Home Security

IoT (Internet of Things) devices, such as **home routers, phone microphones, webcam videos, home sensors**, and **kitchen appliances** pose a big security threat, and are becoming the new cyber attack landscape.

Due to the fact that the Internet has bridged the distance and geography gap between all the world's citizens, now we can be attacked by criminals from any country in the world!

Furthermore, in the last 20 years, we can say that most **computers and smartphones have gone online**. But moving forward, soon enough ***everything*** that is simply **connected to electricity** will be online!

There are a large number of issues when it comes to all of these new online IoT devices:

- Home users believe that their devices are *"secure enough"* when they purchase them
- Home users think their home networks are *not important enough* to be hacked
- However, these IoT devices are sold with:
    - Most features turned on by default
    - Default settings that are difficult or impossible for users to change
    - Outdated software and firmware
        - Firmware is a small piece of code on your IoT device, that makes your hardware work and do what it was manufactured to do
        - Firmware is not usually auto-updated which is one of the biggest problems
    - Default user IDs/usernames and passwords *that are widely known on the Internet* (most people don't change these passwords either)
- Most IoT companies are 10-20 years behind when it comes to implementing security into their IoT products
    - Security is not considered when developing a lot of their firmware code
- IoT devices have no visible screens, so laypeople do not find them easy to manage
    - They are not easy to patch/update as a result
- People want to buy cheap IoT devices, but usually cheap products mean little security was built into the product

IoT MALWARE

Our home routers are HUGE targets for IoT malware and botnets. They are hacked into, and then used to create large "botnets" of hundreds of thousands of systems that are controlled by the hacker. These sys-

tems are subsequently commandeered to cause denial of service attacks against websites, or used for *eavesdropping and surveillance purposes by nation states!*

IoT Mitigation

As a society, we need serious IoT regulation from the government and established institutions. But until that happens, please follow these guidelines for all your IoT devices:

- Any IoT device you buy or install in your home should be secured. These could be:
    - Smart toothbrushes
    - Home routers
    - Smart toasters
    - HVAC systems
        - *Anything with the word "smart" in it!*
- Secure your home routers in the same way you would a computer
    - Remember: they run an operating system in the same way computers do
    - **Change the router's username/password** as soon as you buy it
        - Most IoT devices come with very basic, easy-to-guess passwords like "admin" or "1234password"
    - Change the router's **broadcast SSID** (its network name) so it doesn't have a default name that is easily recognizable by the bad guys
    - Most home routers unfortunately don't have **automatic updates**, which is very frustrating! ☹
        - But if they have this feature, definitely use it!
        - Check the router manufacturer's website to ensure it's running the latest firmware version
            - Set calendar reminders for yourself to do the patches every three months!
        - It's also prudent to reboot your router every three months to flush out any hidden malware that might be installed in the firmware
- **Turn off** the following functions if you see them in your settings:
    - uPnP remote management
    - Remote web admin
    - Port forwarding
    - Telnet, Ping, FTP, SMB
- **Turn on the logging feature**
- **Disable Wi-Fi Protected Setup (WPS)** and set up the WiFi security settings yourself
- **Use the strongest encryption protocol** available today, which is WPA2 PSK:
    - For the WPA2 password make sure it is *16 characters*
- **Change the router's default DNS servers:**
    - "DNS" is basically a service that allows your computer to find websites on the Internet using the full written domain name e.g. Disney.com
    - For your home systems, Cisco offers free DNS servers, called OpenDNS, which have many filters for blocking pornographic and malicious websites
        - You can register your IP address with OpenDNS by following these instructions: https://use.opendns.com/

- It is also prudent to **replace your home router** every three years
- Use a service such as the free **Shields Up Scanner**, which checks how exposed your home computer network may be to the Internet:
  https://www.grc.com/x/ne.dll?bh0bkyd2

What Else Can You Do to Protect Yourself?

Here are a number of safe computing tips you can follow at home (and some good tips for work also):

GENERAL TIPS

- **Be very paranoid on the Internet, and do not trust anyone, even close friends and family**
- It's imperative that you **patch/update the following:**
    - Your operating system
    - All apps
    - Your browser
    - Any add-ons/extensions/plugins in your browser
- Turn on **automatic updates of your operating system and all apps** whenever possible!
    - If this option is available, you should enable it – EVERY TIME!
- VERY IMPORTANT: INSTALL ONLY ESSENTIAL MOBILE APPS, EXTENSIONS, ADD-ONS, PLUGINS AND SOFTWARE!
    - **Uninstall any applications you don't use anymore**
    - Remember: every application you install is a **new way into your system for a hacker**
        - Think of each new application as a window that's left open in your house
    - For Windows systems at home, you can install **SUMO, uCheck, CCleaner Premium, Patch My PC Home Updater,** or **File Hippo** to scan and update your apps automatically
    - **https://patchmypc.com/home-updater-download**
    - **https://filehippo.com/download_app_manager/**
        - Keep in mind that some antivirus programs these days can also search all your installed applications for updates e.g. Kaspersky, Avast
    - For Apple systems at home, please follow the instructions in the **"Mac Security"** section
    - At work, please allow your IT teams to handle the automatic updates of your system for you

JAVA TIPS

The *"Java application"* is installed on most computers, and is a *VERY common way for the bad guys to attack a system connected to the Internet*

- Java is a widely installed and powerful software package used to run certain interactive applications, games etc. and can plug straight into the browser
    - ***NOTE: Java** and JavaScript are very different*
- Now it's being replaced by HTML5 which is native to your browser, so you don't need an extra plugin for it
- Because JAVA has so many security holes in it, it requires frequent security patching
    - **If you do not require Java, remove it immediately from your system, or at least remove the Java browser plugin**
    - **Java should always be updated to the latest version if you need it on your system**
        - You can find out if you have Java installed and which version here:

          https://java.com/en/download/help/version_manual.xml

        - Mac users are safer with respect to Java, because Apple has disabled the Java browser plugin by default ☺
        - *NOTE: The NoScript plugin will, by default, block all Java applets and Flash content from running*

    - *At home, if you wish to remove Java from your system, please refer to the following useful guides:*
        - *ON WINDOWS:*
            - ***https://www.java.com/en/download/help/uninstall_java.xml***
            -
        - *ON MAC:*
            - ***https://www.java.com/en/download/help/mac_uninstall_java.xml***

- Use an add-on like **NoScript**, or **Script Safe** to block malicious JavaScript
    - NoScript does take a little getting used to, but be patient, and it will serve you very well ☺
    - First, in the settings, disallow JavaScript from running on all websites by default
        - Then selectively enable the scripts as needed on each website domain you visit
        - *(You can do this permanently or temporarily for a single browsing session)*
    - It will take a few days for you to *train* your script blocker to know which websites you trust and normally visit
        - If you really trust a reputable site, you can turn on just the script for the actual website domain to run permanently
        - Because it may be a bit complicated at first to use, if you are not sure about turning each and every script on or off, you may opt for the worst case which is to turn on all scripts temporarily/permanently for that site
        - Please note this is risky because even benign websites can be hacked and serve malicious content, or serve malicious ads
        - When you block all scripts, many times you might notice broken functionality on the website. If so, you can selectively turn on each script you feel may be the culprit, until it starts working
        - IMPORTANT: for all the untrustworthy websites you may visit, block all scripts by default, and do not allow any or all scripts to run unless you absolutely have to
            - This will prevent any malicious scripts from running on your system when you accidently visit a malicious website!
            - Here are a few good resources that explain how to use NoScript:
              https://www.youtube.com/watch?v=UhJTwCFFzrE
              https://www.youtube.com/watch?v=AC4ALEKZRfg
              https://blog.jeaye.com/2017/11/30/noscript/

==========

VERY IMPORTANT TO NOTE:

REST ASSURED THAT IF ANY WEBSITE YOU ARE VISITING IS NOT WORKING, DO NOT BE FRUSTRATED! YOU CAN ALWAYS GO INTO NOSCRIPT/UBLOCK ORIGIN/GHOSTERY/PRIVACY BADGER ETC AND EITHER **DISABLE BLOCKING FOR THAT SITE**, OR TELL THE ADDON TO **TRUST THE ENTIRE SITE**. IF THE BLOCKING OF SCRIPTS OR TRACKERS WAS THE CAUSE OF THE BREAK IN FUNCTIONALITY, YOU CAN ALWAYS REVERT BACK TO THE ORIGINAL STATE OF THE WEBSITE WITH LITERALLY 1 CLICK

==========

- **Uninstall all unneeded web browser plug-ins/add-ons/extensions**
    - There are many Chrome/Firefox extensions and addons that will compromise your computer or laptop, or collect your private data
    - You can run **Qualys Browser Check** to see which extensions need updating or removal: https://browsercheck.qualys.com/

ANTIVIRUS TIPS

At home, have a current antivirus program running on your system at all times!

- Set it to automatically update itself every day

- Set it to check **all** files automatically, including USB thumb drives

- Microsoft has a decent built-in antivirus solution in Windows 10 called **Windows Defender:**
    - You can use the free Windows Defender + commercial MalwareBytes
    - **Windows Edge Browser + Windows Defender + Office 365** together are very good at fighting ransomware and phishing emails

- **Microsoft's O365 ATP** has become very effective at blocking phishing

- Microsoft's built-in & commercial **Windows Defender umbrella** is also worth looking at if you want *complete* end-point protection:
    - **Sophos, Bitdefender, Avast** and **AVG** offer free virus detection software for Windows
    - *NOTE: For Windows systems, it is worth it to purchase a commercial antivirus program for added protection*
    - **McAfee, Symantec, Trend Micro, Bitdefender** and **ESET** are good commercial editions for Windows systems

- **Sophos Antivirus** is a great free solution for Apple Macs

- If possible, buy a cutting-edge antivirus solution that includes machine learning in its detection capabilities
    - **Cylance is one example**
    - *(Machine learning is a form of computer artificial intelligence that helps the antivirus program learning by analyzing data and identify recurring patterns)*

- For small-to-medium businesses consider **CrowdStrike Falcon Endpoint Protection Complete,** which includes the endpoint security module of the Falcon X platform
    - They also offer dedicated incident response security professionals to assist in the unfortunate event of a data breach

Malware Bytes Premium

- It can work alongside antivirus software as it uses a different strategy:
    - Antivirus software will stop malicious programs that install on your computer
    - Malwarebytes will try to stop malicious programs from even reaching your computer in the first place
        - Malwarebytes has free and premium versions for Windows and Mac
        - We recommend you purchase the commercial version

Malwarebytes Browser Extension

- Blocks malicious sites, popups, tech support scams
- Has ad and tracking blocker
- Keeps an eye on your plugins and extensions for any malicious activity

Malwarebytes for iOS App

- The app includes call and spam blocking, protection against web browser threats, message filtering etc.
- It also contains anti-ransomware

Mobile Antivirus

- **Sophos, Bitdefender, Trend Micro, McAfee, Mobile Security** and **Lookout** all have free and commercial versions of antivirus for the Android and iPhone. For reasons stated in the "Mobile Security" section, please install an antivirus program on your Android for added protection

What to Do If You Suspect Your Home Computer Has a Virus

- Immediately stop shopping, banking, and other online activities that involve user names, passwords, or personal data
    - Assume that your various account names and passwords have now been stolen
    - Locate a safe computer or mobile device and change your online passwords, especially for financial or credit card accounts
    - Monitor your accounts for unauthorized activity or fraud

- Immediately disconnect your machine from your home or work network by pulling the network cable out of the back of the computer!

- Confirm that your security and virus detection software are up to date

- Then use the virus detection software to scan your computer:
    - Review the problems it identifies and follow directions

- You may run a second virus detection tool or contact professional help:
    - Many times, malware is very difficult to remove because they bury themselves deep into the operating system

    - *It is strongly recommended that you re-install the operating systems and copy your data from a backup drive in the event of a malware infection*

- Have individual user accounts to use, versus using the administrator account for normal day-to-day computer activities
    - Use your normal user account for most of your work at home such as browsing, gaming and document editing
    - **Only use the administrator account to *configure the system or install new software:***
        - *By using only your regular account for everyday tasks, if your system is compromised by malware, the malware would usually only have limited access to your files and the overall damage may be reduced*

- If possible, restrict sharing your file system, and disable any kind of remote access or desktop services such as RDP (Remote Desktop Protocol):
    - RDP is very popular in spreading ransomware and other types of malware. If you have to use RDP, make sure you:
        - Use strong passwords
        - Use 2FA
        - Update to the latest version of RDP
        - Restrict access to the default RDP port
        - Enable logging for all RDP logins

- Have a firewall and set it to inspect *both* **inbound** and **outbound** connections

- Back up important files regularly with automated backups
    - Storage costs are *extremely* cheap so we have no excuses!
    - Always have TWO copies: one local external drive and one in the Internet cloud! (Dropbox, iCloud, Box, Google Drive)

- Ask your manager for the proper procedures to handle your company data and to be compliant with company policies

- At no time should you provide your user account name and password to anyone:
    - Not even IT or Security staff, or family members

- Take care not to work in an area or manner where unauthorized persons may see company data

- Ask your IT or Security department to dispose of unused computer media or computer equipment

- Report concerns and suspected security incidents to **your IT or Security department ASAP!**
    - Please do not investigate security incidents on your own
    - Examples of events to report:
        - System alerts such as virus detection, system or application failure or disruption
        - Unauthorized hardware or software changes or additions
        - Unauthorized system or data access or unauthorized use

- **If your company policy dictates that you store their data in the cloud, make sure you are protecting the data both when it is sitting on your computer, or if you are sending it over the Internet to a client or colleague**
    - Don't only rely on secure web *SSL* connections when you are copying data into the cloud
        - Make sure you have strict policies to protect the data when it is stored in the cloud as well!
        - If your cloud permissions are even slightly misconfigured, it may expose the entire data set to the whole world
        - If in doubt, work with your IT department to ensure any cloud storage or buckets you are using are not misconfigured to expose them

==========

The following tips are from a well-respected security researcher named Brian Krebs, who maintains a popular security blog called "Krebs on Security."

He has created "Krebs's 3 Basic Rules for Online Safety"[3]:

- ***Krebs's Rule #1: "If you didn't go looking for it, don't install it!"***
- ***Krebs's Rule #2: "If you installed it, update it!"***
- ***Krebs's Rule #3: "If you no longer need it, remove it."***

[3] *https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/*