

SPIES, INTRUDERS AND SURPRISES..

Oh my!!

WHAT WE ARE GOING TO DISCUSS

- Useful Sites to visit.
- Your passwords how safe are they?
- Are you just being social or socially engineered?
- How safe is your email?
- 5 excuses not to use security
- Did the horse get out of the barn? Physical Security
- What is PII?
- Mobile devices are they safe
- Reporting activity
- WiFi is it always safe and why we use it

RECOMMENDATIONS FOR THIS SESSION

- Open discussion
- Refrain from online banking and purchases
- Don't login to websites you do not want to be revealed.
- Basically limit you online activity (if you can)

Now we can continue



USEFUL SITES TO VISIT

- [NakedSecurity](#)
- [The Hacker News](#)
- [SANS Internet Storm Center News](#)
- [Identity Theft Resource Center - ITRC](#)
- [Verizon – 2015 Data Breach Investigation Report](#)
- [US-CERT Current Activities](#)
- <https://haveibeenpwned.com>
- <https://www.virustotal.com>

PASSWORDS

So, ask yourself this...

- Do you use the same password for both work and personal sites?
- Is your password long and complex?
- Do your password(s) expire or do you change them?
- Do you share your passwords?
- Do you write them down, are they taped to the bottom of my keyboard, desk or just saved to my computer in a file?

PASSWORDS (SIMPLE RULES TO FOLLOW)

- Never share your passwords
- Make sure they are long and complex
- Expire 60-90 days
- Never use the same passwords
 - Work
 - Personal
 - Every web site, email address, resource, etc.

**PASSWORD MUST CONTAIN
8 CHARACTERS WITH ONE CAPITAL, AND
ONE SPECIAL CHARACTER**

"MickeyMinniePlutoHueyLouieDeweyDonaldGoofySacramentoDopey"



PASSWORDS

- iPhone lock screen usually is 4 numbers – 4672
- iPhone OS9 lock screen will allow 6 numbers -467230
- A lot of passwords must be at least 8 characters long with one number, capital and special character – Silly1duck!
- However, when it comes to passwords most of the time the longer the password the better.
- Like rowrowrowyourboat or RowRowRowRowyourboat. Even better would be R0wrowr0wyourB0@t.
- [How strong is your password](#)

PASSWORDS

- **What is Password Cracking?**
 - Password cracking is the process of guessing or recovering a password from stored locations or from data transmission system. It is used to get a password for unauthorized access or to recover a forgotten password.
 - However, hackers don't have to hack you, your credentials may already be posted on the internet on a site like this:
<https://twitter.com/dumpmon>
 - During this discussion we will demo one method

PASSWORDS

- DEMO password cracking tool -Hashcat
- Have you been compromised: <https://haveibeenpwned.com>

ARE YOU JUST BEING SOCIAL OR SOCIALLY ENGINEERED

So, ask yourself this...

- Do you or your children use social networks?
- What kind of info is out there our there?
- Do I let others know where I am at?
- Do you really know the person that you friended?
- Are the files and links sent safe? Do you open them?
- Do you monitor your children's accounts?

ARE YOU JUST BEING SOCIAL OR SOCIALLY ENGINEERED

- Harvesting Social Networks
- Too much information online today
 - Professional information
 - Personal information
 - Family
 - Hobbies
 - Location
 - Charity/volunteer
 - Likes/dislikes



Aggregate information can be assembled for a detailed profile

ARE YOU JUST BEING SOCIAL OR SOCIALLY ENGINEERED

- Social media
 - Facebook, LinkedIn, Instagram, Google talk, YouTube, Pinterest, Twitter, Snapchat any of your favorite site(s) you visit, etc.
 - Be aware what kind and how much info you provide to these types of sites.
 - Understand the person(s) you might be friends with might not be who you think it is
 - Be aware links, games, pictures, videos, etc. could carry a payload.

ARE YOU JUST BEING SOCIAL OR SOCIALLY ENGINEERED

- Email
 - Email is great when used as it was intended however, it is also used frequently by individuals that want to steal your data and/or personal information.

ARE YOU JUST BEING SOCIAL OR SOCIALLY ENGINEERED

So, ask yourself this...

- Are all emails safe?
- Are you sure the sender is who they say they are?
- Should I click the link or attachment in this email?
- Should I click this tiny url (link), wonder where it goes?
- Should I verify the sender before I open the link or attachment?

5 EXCUSES FOR DOING NOTHING ABOUT COMPUTER SECURITY!

BY PAUL DUCKLIN ON AUGUST 20, 2014

- Let's be honest: computers and websites are often easier and quicker to use if you do nothing about security.
- So, here are five excuses that we hear a lot, both from individuals and from small businesses.

**EXCUSE 1.
NO-ONE'S INTERESTED IN LITTLE OLD ME!**

- The reasoning is that cybercrooks just aren't interested in the local automotive repair shop or cake-making business, because...
- ...well, why would they go after an individual earning \$30,000 per year, or a local business turning over \$500,000, when they could take on a retailer like Target with annual sales of \$70,000,000,000?
- But stop to think for a moment: Target doesn't turn over \$70 billion a year by closing 70 deals of \$1 billion each.
- Target's business is much more like one billion transactions of \$70 each.
- And many cybercrooks run just that sort of low-value/high-volume business.

We're all in the sights of cybercrooks somewhere, and we owe it to ourselves and to everyone else to do the best we can to thwart them.

**EXCUSE 2.
MY PRINTER WON'T WORK WITH THE LATEST UPDATES.**

- OK, it's not always a printer that gets the blame; in fact, it's not always hardware.
- Sometimes it's legacy software that provides the excuse for sticking in the mud of yesterday's insecurities.
- If you have a security hole that criminals have already had months or years to hone their skills against, they're going to attack you first, because they already know how to break in.

Every time you fall further behind on security updates, you make yourself into lower-hanging fruit for cybercrooks.

**EXCUSE 3.
I'VE GOT A MAC.**

- Whatever sort of computer you have, and whatever operating system it's running, if it is ever lost or stolen then your data will be in someone else's hands.
- You have to remember that your data has underground value, too, even if only in the form of a bulk "data dump".
- In short, computer brand choice alone simply isn't enough to keep your data safe.

Don't leave home without full disk encryption, so that the only data dump a crook will get is shredded cabbage.

**EXCUSE 4.
SECURITY SLOWS YOUR COMPUTER TO A CRAWL.**

- Full disk encryption, for example, sounds as though it ought to make your computer slow, because it has to unscramble everything it reads in, and rescrumble everything it writes out.
- Anti-virus often gets a bad name, too, but we very often find that it only genuinely gets in the way when people needlessly "flip all the switches," turning on redundant combinations of scanning options that do more work than is necessary.
- Similarly, strong passwords and two-factor authentication are often blamed for making software and web sites time-consuming to use, even though they typically add just a few seconds to important transactions.

Don't throw out security altogether to save a little bit of time today, because it could end up costing you many times over tomorrow.

**EXCUSE 5.
I ONLY BROWSE TO SAFE SITES.**

- Do you? Really?
- The thing is, how do you know?
- How can you tell in advance that a site is safe?
- Remember that even legitimate and high-profile sites may put you at risk, for example because they include poisoned adverts from a third party provider that was hacked.
- That's where web filtering technology can help, because a good web filter not only examines the URLs of the web pages you plan to visit before you even go there, but also checks out the content of web pages you've fetched before they are processed by your browser.

Don't assume that all online cybercrime is obvious, even if you're visiting sites that were just fine yesterday.

**ARE YOU JUST BEING SOCIAL OR
SOCIAALLY ENGINEERED**

- DEMO
- SET – Social Engineering Tool kit
 - Real life phishing demo

PHYSICAL SECURITY

Home	Work
Lock your doors when you leave	Lock your computer when you leave and lock your office.
Make sure all your belongings are secure: keepsakes, jewelry, guns, etc.	Make sure all data is secure
Be aware of your surroundings 1) Watch after your neighbors 2) Watch for strangers 3) Report unusual activity	Be aware of your surroundings 1) Watch after your fellow workers 2) Watch for strangers 3) Report unusual activity

PHYSICAL SECURITY ACCESS



**PHYSICAL SECURITY
EXPOSED NETWORK CONNECTIONS**



**PHYSICAL SECURITY
TOO MUCH INFORMATION**



PHYSICAL SECURITY CAMERAS, DO THEY REALLY WORK OR EVEN MONITORED?



PII (PERSONAL IDENTIFIABLE INFORMATION)

So, ask yourself this...

- Do I know what PII is?
- Do I have PII data in my possession? If so where?
- How do I make sure it's safe?
- When a request is made should I share it?
- If PII is lost or stolen how do I report it?
- [Who is responsible for our PII in our department.](#)

PII (PERSONAL IDENTIFIABLE INFORMATION)

- **Personally identifiable information (PII)**
 - PII - is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
 - Keep all PII Documents under lock and key
 - When asked for PII information, it is OK to question the requester as to how they are going to keep it safe and why it is needed. Get it in writing.
 - Always follow all policies and procedures within your division or agency when it come to PII.

MOBILE DEVICES AND SECURITY

So, ask yourself this...

- Do I know where my mobile devices are?
- Do I have a password on it?
- Do you try to store important info on it in notes or even in your contact list?
- If I lost my phone do you know who to call to have it shutdown or located?
- Do I keep it on me at all times?
- Is the free app you just downloaded safe, what kind of info is it sending out and to whom?

MOBILE DEVICES AND SECURITY

- Mobile Devices
 - **What about Mobile Apps?**
- Unlike websites, mobile apps don't have a visible indicator like **https**. Researchers have found that many mobile apps don't encrypt information properly, so it's a bad idea to use certain types of mobile apps on unsecured Wi-Fi.
- If you plan to use a mobile app to conduct sensitive transactions — like filing your taxes, shopping with a credit card, or accessing your bank account — use a secure wireless network or your phone's data network (often referred to as 3G or 4G).
- If you must use an unsecured wireless network for transactions, use the company's mobile website — where you can check for the **https** at the start of the web address — rather than the company's mobile app.

MOBILE DEVICES AND SECURITY

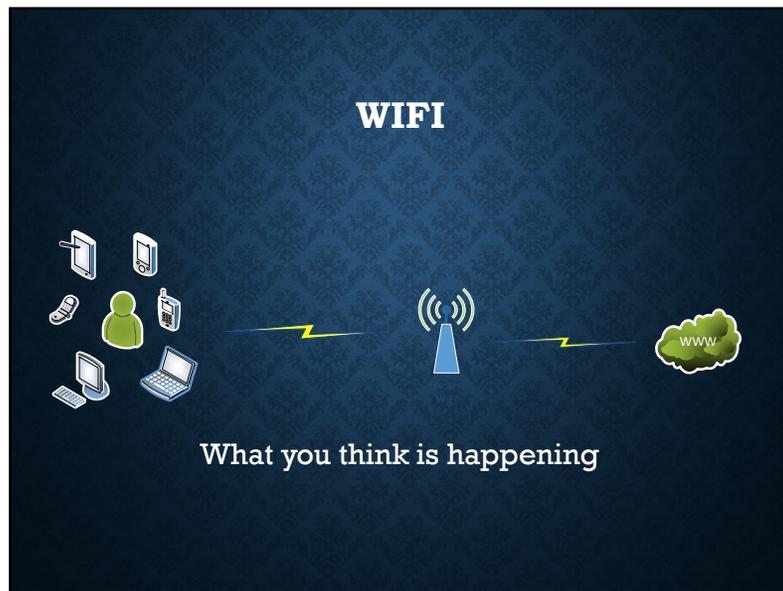
- Demo - SMS phishing attack

REPORTING SUSPICIOUS ACTIVITY

- **Reporting any and all incidents or suspected incidents.**
 - **Make sure you know who to report your incident to.**
 - **Try and document as much information as you can to assist with the investigation.**
 - **When it comes to reporting an incident there is no such thing as crying wolf.**

WIFI

- **Is Wi-Fi really safe?**
 - **Wi-Fi terms**
 - **SSID – Service set identifier**
 - **WEP – Wired equivalent privacy**
 - **WAP – Wireless application protocol**
 - **WPA2 – Newer version of WAP**
 - **Let's see**
 - **Reading material**
 - <http://www.pcworld.com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now.html>
 - <http://www.pcmag.com/article2/0,2817,2420002,00.asp>
 - <https://www.onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks>



WIFI

- DEMO

THE EASIEST WAY TO PROTECT YOURSELF AT EITHER WORK OR HOME

- Make sure ALL your software is up to date.
- Use two factor authentication when you can.
- Use long complex passwords and use different passwords for every site.
- When using social networking be cautious.
- Make sure when you get an email it is legit before opening any attachments or links.
- Remember even trusted internet sites can and will be compromised. Be cautious when surfing.
- If you lock your doors when you leave home or car you should treat your computer or electronic device the same way.
- Keep all your personal identifiable information safe.
- Mobile devices are pocket computers they can be compromised and leak as much if not more data about you so keep them protected.
- Reporting activity – don't be afraid to take a chance even if you think its nothing
- WiFi is safe as long as you understand that who you are connecting to is legit. Don't just join any wifi connection.

FINIAL ADVICE

- ***Remember that security is everyone's responsibility.***

- *Make it hard for the bad guys – be the fruit at the top of the tree not on the low hanging branches.*
- *If you protect yourself you will be protecting your family, friends and co-workers too.*
- *It starts with you and ends with you.*

**DON'T' JUST IGNORE
THE MAN BEHIND THE
CURTAIN.**

Better yet know he is there and waiting to do you and yours harm.