Critical Steps To Avoid Being A Cyber Security Victim

How to secure your information with today's Internet risks

February 22, 2018
David Mandala

Who is David Mandala & What Does He Know?

- I've worked in the Electronics and Computer Industries for 40+ years.
  - I've been with seven startups, the principal of three of them.
- I spent the last 10 years developing embedded computer operating systems or improving them.
  - Ubuntu Linux for ARM System on Chip (SoC).
  - Improving Linux for the ARM SoC's with Linaro.
  - Standardization of the 96Boards platform so that binaries run on any board without recompilation of source code.
- I started **Secured by THEM LLC** to specifically help small businesses secure their business computers and networks.

What is Cybersecurity

Cybersecurity, computer security, or IT security is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

- Wikipedia

Cyber Attacks Occur Daily

Nearly every day you hear about a new cyber crime from credit card theft to personal/business information loss.

- Target
- Chipotle & Pizzeria Locale
- The Buckle Inc. 450 stores hit between Oct. 28, 2016 and April 14, 2017
- Equifax **Credit-Card**-Data Breach Could Be **Largest** in U.S. History
- Yahoo loses more than 1 Billion account records
- In 2016, hackers stole the data of 57 million Uber customers, and the company paid them $100,000 to cover it up. The breach wasn't made public until last November.

Ka ching

- Stolen credit card info, paid for in untraceable cyber currency such as Bitcoin, can sell for anywhere from $5 to $250 each.
- Email addresses (useful for phishing campaigns) sell for $10 to $15 per thousand.
- Online bank accounts in the U.S. sell for two percent of the account balance.
- PayPal accounts can net six to 20 percent of the balance.
- Stolen health insurance information can bring in a whopping $1,300 per record.

According to Havocscope, the global black market price guide.

Easy Things to Avoid

- Avoid using public networks; Hackers love public networks
- Avoid using public computers for sensitive business; Could have keyloggers installed
- Avoid downloading unknown applications
- Do not use pirate software, ie software downloaded from unsafe sources, including torrents and other peer-to-peer file sharing. It is not about morality or ethics – it is simply unsafe.

What to Do?

- Install/Turn on the firewall for your network; Make sure UPnP is turned **OFF**
- Install anti-virus, anti-malware and anti-spyware software; Keep the software active at all times and keep it updated to the most current.
- Encrypt data.
- Backup data regularly.
- Log off and shut down their computers when they are not being used.
- Install OS updates as soon as they become available.

What to Do?

- Keep up to date on major security breaches. If you have an account on a site that's been impacted by a security breach, find out what the hackers know and change your password immediately.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information.
- Use a VPN to Hide Your IP Address, your IP address can tell people geographical data and, with some digging, can be cross-referenced with online activity to reveal a rather disturbing amount of your information.

Credit Card Readers - Stay Alert

- ATM's, gas pumps, any kind of a machine where you slide your credit card into the machine are potentially dangerous.
- Before you insert your card, reach out and pull on the card reader, try to pull it out of the device, see if your fingernails catch on any part of the reader and pull; Try to wiggle everything, real machines are solid, with no loose parts or "wiggle"
- ALWAYS cover your hand with your other hand if you have to enter a pin number. The supplied visual cover is not good enough, cameras are so small they can be pasted on the back of the visual cover!
- If at a gas station and you have any reason to be suspicious go inside and pay the clerk.

Credit Card Readers - Stay Alert

Credit Card Readers - Stay Alert

If you have an android phone download and install the “Skimmer Scanner” app it will spot some types of skimmers, but not all of them.

Web Browsing and Staying Secure

- Set your browser security high enough to detect unauthorized downloads
- Limit the use of browser plugins. Disable commonly exploited ones such as Flash Player and Silverlight when you're not using them. You can do this through your web browser under the plugin settings.
- Use a pop-up blocker (the links in pop-up ads are notorious sources of malware)
- When filling out personal information on a site, make sure they aren't asking for your social security number or excessive financial information. Both are telltale signs of a fraudulent website.

Web Browsing and Staying Secure

- Whenever possible use a credit card when paying for something rather than a debit card. Credit cards have limits on what you can spend whereas debit cards are tied directly to a bank account. Make sure and review your statements, to see if there are any unauthorized charges. If there is a discrepancy, it's important to report it immediately.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- When using websites that take info from you make sure they are using secure traffic layers (SSL) so the URL should start with https:// the **s** shows it is secure. Never provide information of any kind to a website that only uses insecure traffic layer: http://.

Password Do’s & Don’ts

- Use strong passwords, long and random are best but hard for humans to remember.
- Do not share or give out your passwords.
- Do not re-use old passwords.
- Implement an employee password policy.
    - Use password vaults (PV), perhaps buy employees a subscription to one as a perk? If you supply it you can require that employees use the password vault for all work related passwords, if you do that, require 70+ character random passwords be used for all work related items (unless some stupid websites force shorter passwords).
- Don’t use the same passwords on different websites.

Password Do’s & Don’ts

- Here again a PV is your friend and is a strong perk for employees. It’s trivial to have long random passwords for every site you use with a PV.
- Opt for 2-step verification whenever offered:
    - The 2-step verification (2FA) system means that stealing your password by itself won’t be enough. Once you enter your password, the system will send a notification to your e-mail or phone with an additional code in it, or you have a token generator on your phone. You will have to enter this code to access your account. While it’s not impossible for a thief to get this information, hacking becomes much more difficult and less likely.

Your Pocket Computer

- Don’t trust caller ID, worthless anymore
- Don’t trust text messages, (same problem as caller ID)
- Install anti-virus, anti-malware and anti-spyware software. Keep the software active at all times and keep it updated to the most current.
- Avoid using public WiFi.
- Your devices battery life is suddenly and drastically shortened! Malware or a virus could be running.

The IoT - Home/Work Automation

The Internet of Things (IoT) are devices that are useful, do things for you and have an embedded computer in them. Items such as video doorbells, thermostats, home audio/video devices, smart TVs, Google Home, Alexa, really any device that connects to Ethernet or WiFi to do something for you.

These devices:

- Generally lack security.
- Will upgrade themselves when they want to or not.
- Should **NEVER** be connected to your main home/office network..
    - WiFi devices should be on a Guest network,
    - Ethernet devices should be on an isolated network, either vlan or totally separate from your primary network. Yes this will take some work to set up.

SOME Smart Devices Available

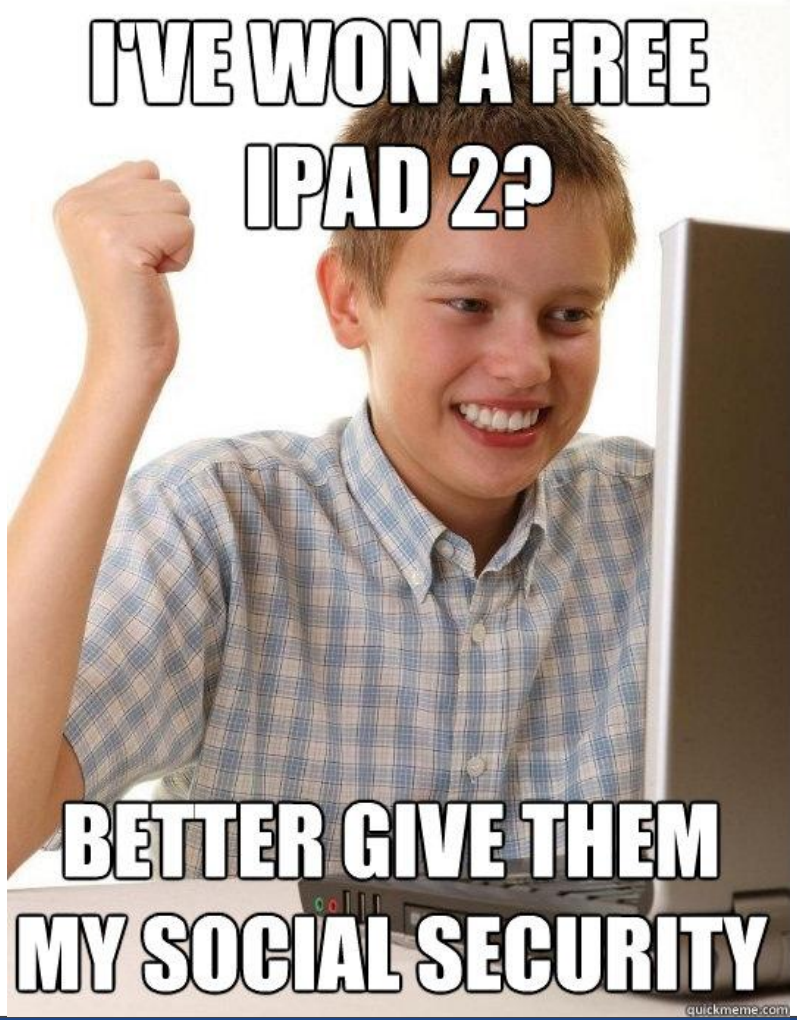
There are more more than **43 classes** of IoT devices sold on Amazon alone:

- Smart Lightbulbs
- Smart Locks
- Smart Wall Plugs
- Smart Light Switches
- Smart Wall Touchscreen
- Smart Thermostat
- Smart Garage Door Opener
- Smart Blinds
- Smart Curtains
- Amazon Alexa
- Amazon Dot
- Smart Keyrings
- Smart Egg Minder
- Smart Blu-Ray Player
- Smart TV
- Smart Outdoor Switch/Plug
- Smart Trackers (keys, luggage, etc)
- Smart Speakers
- Smart Cameras (security)
- Smart Alarm Systems
- Smart Pet Feeder
- Smart Smoke Detector
- Smart Carbon Monoxide Detector
- Smart Air Quality Detector
- Smart Landscape Lighting
- Smart Home Controller
- Smart Doorbell
- Smart Pet Treat Feeder / Camera
- Smart Weather Station
- Smart Plant Watering Device
- Smart Garden Sensors
- Smart Picture Frames
- AeroGarden with WiFi
- Smart Plant Pots
- Smart Sprinkler Controller
- Smart Crock Pot
- Streaming Media Player
- Smart Coffee/Tea Pot
- WiFi Video Projector
- Smart Robot Vacuum
- Smart Range
- Smart Microwave
- Smart Dishwasher

Ransomware

Petya, WannaCry and NotPetya are all strains of ransomware that affected the computer systems of organisations worldwide. Ransomware is a type of malware that is delivered by social engineering and blocks access to the information stored on your device/system. Users will be denied access to their information unless they pay a ‘ransom’ to the attacker – usually in an electronic currency such as bitcoin.

If you are doing your backups regularly ransomware is an annoyance at best, no backups? Now you have a problem…..



Don’t Fall for Phishermen

The attacker tries to manipulate you into giving them either your information, or access to your computer so that they can get the information themselves. This can take place through many types of communication, including the telephone (vishing), email (phishing), text messages (smishing) or chats within games or apps. The aim of social engineering is to exploit human nature by targeting common human traits such as the fear of being attacked.

Don’t Assume Any Email is Legitimate!

If you get an email that appears to come from a company you know, and it says that you owe money or you need to click HERE to verify your account **DON’T DO IT**.

This is an example of a **Phishing Email**.

These emails falsely claim to be from legitimate vendors and typically try to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information.

A good rule of thumb is to not click any links in an email. Instead go to the site by typing the address into your browser, or call the phone number on the company website. You can then verify if the email was legitimate.

It’s an Easy Trick

Criminals frequently send email that appears to come from someone you know. They’ll disguise malicious software as images or documents attached to these email messages.

Word to the wise: You should never open or download email attachments from any email without (1) expecting the information or (2) confirming with the person that supposedly sent it to you.

So how can customers know email is really from me?

Use a Secure Email certificate, this adds security and authenticity to your email communications. Encryption keeps your email private, digital signing ensures the integrity and authenticity of the message. It's easy to have all email from your company signed.

https://www.comodo.com/e-commerce/email-certificates/email-privacy.php

WiFi

WPA2 security on WiFi networks is no longer secure, in fact, you can't trust it!

All traffic over WiFI must be secured via an additional method. SSL for web, SSH for other file transfers, encryption for any files leaving your system.

Don't allow anyone to use your WiFi at the office or home: Create a separate guest network with a strong password and allow people to use that only.

Uh-oh, Now What?

If the worst should happen and your company suffers a natural disaster, data breach or similar attack, you should have a **Business Continuity Plan** in place.

A **Business Continuity Plan** should identify potential risks, along with the recovery team at your company assigned to protect personnel and property in the event of an attack. The recovery team should conduct a damage assessment of the attack and guide the company toward resuming operations.

Uh-oh, Now What?

A **Business Continuity Plan** will:

- Facilitate timely recovery of core business functions
- Protect the well-being of employees, their families and your customers
- Minimize loss of revenue/customers
- Maintain public image and reputation
- Minimize loss of data
- Minimize the critical decisions that need to be made in a time of crisis

Last but not least!

LOCK your credit report, this should have been done months ago but if you have not done it yet, get it done ASAP.

- TransUnion - https://www.transunion.com/
- Equifax - https://www.equifax.com/personal/
- Experian - http://www.experian.com/

I Listened, I Must Be Secure

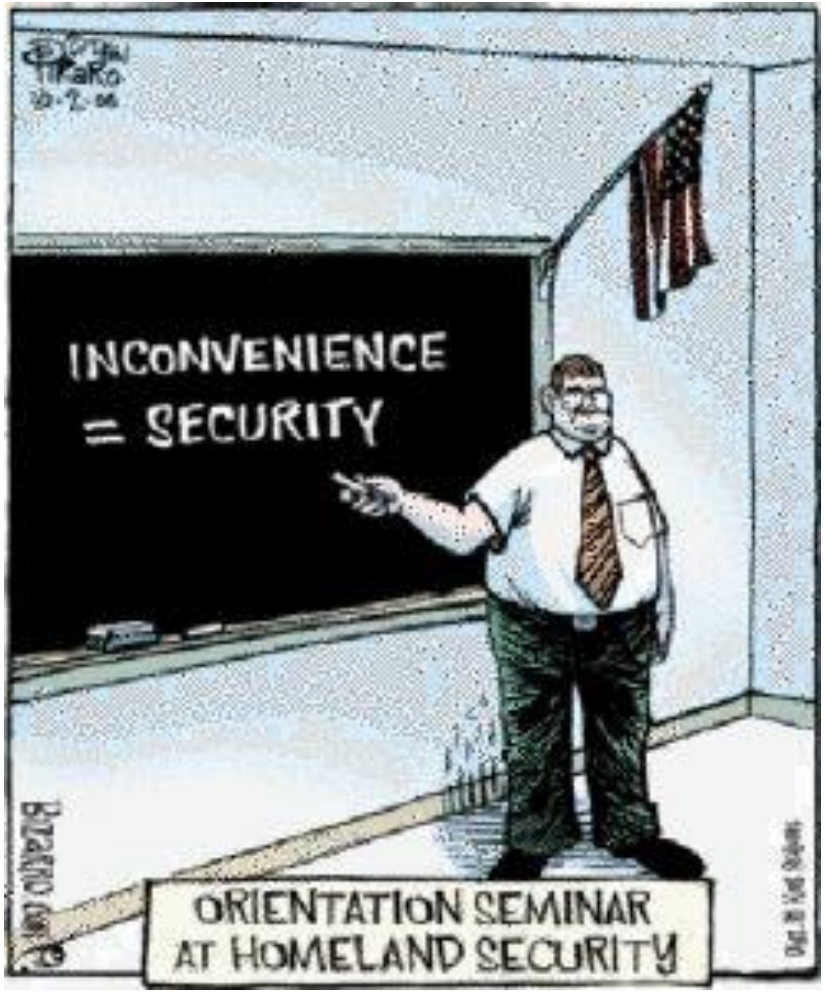
Even if you do everything I suggest, being 100% securite is not possible.

You will certainly be more secure than before, but the truth is this presentation only scratches the surface. **There is no such thing as a completely secure device, only levels of security.**

Security is like an onion, the more layers you have the more secure you are.

Everyone’s situation is unique, and must be addressed individually.

Feel free to reach out and talk with me. (info@them.com)



Questions?

Reference Links

Credit Card Readers:

https://www.engadget.com/2014/07/28/credit-card-skimming-explainer/

https://krebsonsecurity.com/all-about-skimmers/

Password Vault:

https://www.lastpass.com

https://www.roboform.com/

Whole disk encryption:

https://www.veracrypt.fr/en/Home.html

https://www.microsoft.com/en-us/store/d/windows-10-pro/df77x4d43rkt/48DN

Comparsion of veracrypt and bitlocker: http://lifehacker.com/windows-encryption-showdown-veracrypt-vs-bitlocker-1777855025

Reference Links

Secured by THEM

https://www.them.com/

info@them.com

(469) 298-8436

Thank you for your time.

February 22, 2018
David Mandala

WHO'S ON YOUR NETWORK?