Cyber 101 Training for SMB Execs

Cybersecurity 101 for Government Agencies and Contractors

NetWatcher

62% of Cyber Attacks are aimed at Small Business

– Verizon Cyber Crime Survey

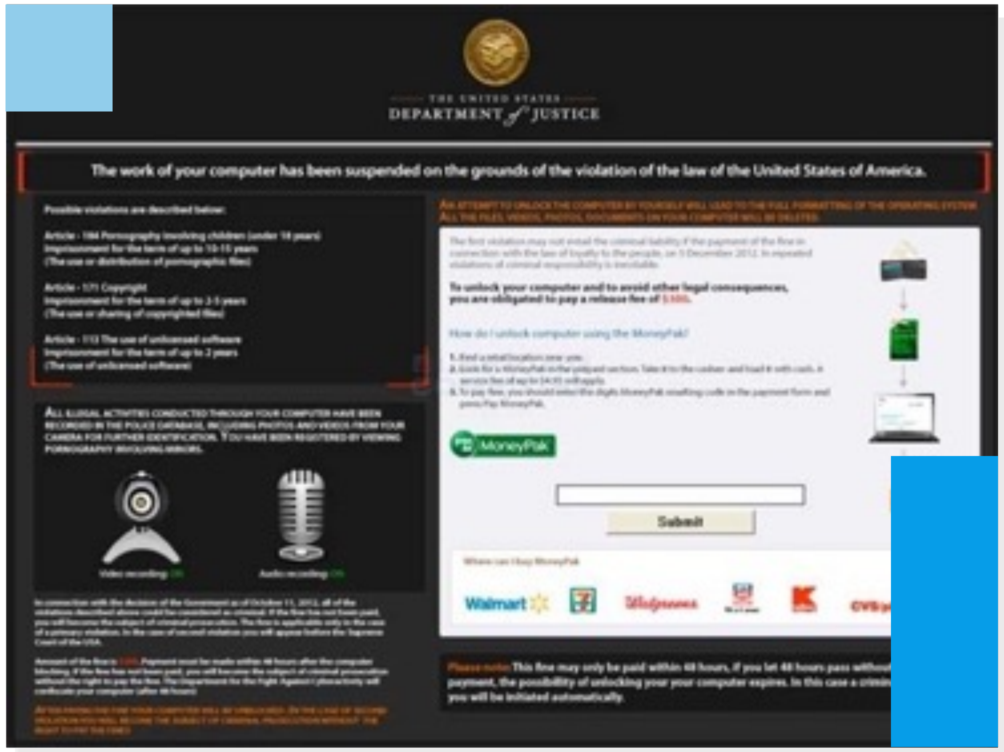
>50% of small-to-medium sized businesses had experienced at least one data breach

– Ponemon Institute

What Are They After?

- Money – Ransom-ware
- Your company’s data
  - Personally Identifiable Info (PII)
  - Protected Health Information (PHI)
  - CC Numbers and/or Financial Info
  - Intellectual property – copyrights, trademarks & patents, business plans, customer lists, etc.

- Your customer’s data & access to your customer’s network…
  - The Target breach happened due to an HVAC vendor – more.



THE UNITED STATES
DEPARTMENT of JUSTICE

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article - 184 Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article - 171 Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article - 113 The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

In connection with the decision of the Government as of October 11, 2012, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the Supreme Court of the USA.

Amount of the fine is [illegible]. Payment must be made within 48 hours after the computer blocking. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against [illegible] will confiscate your computer (after 48 hours).

[illegible]

AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF THE OPERATING SYSTEM. ALL THE FILES, VIDEOS, PHOTOS, DOCUMENTS ON YOUR COMPUTER WILL BE DELETED.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people, on 5 December 2012. In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your your computer expires. In this case a crimin[illegible] you will be initiated automatically.

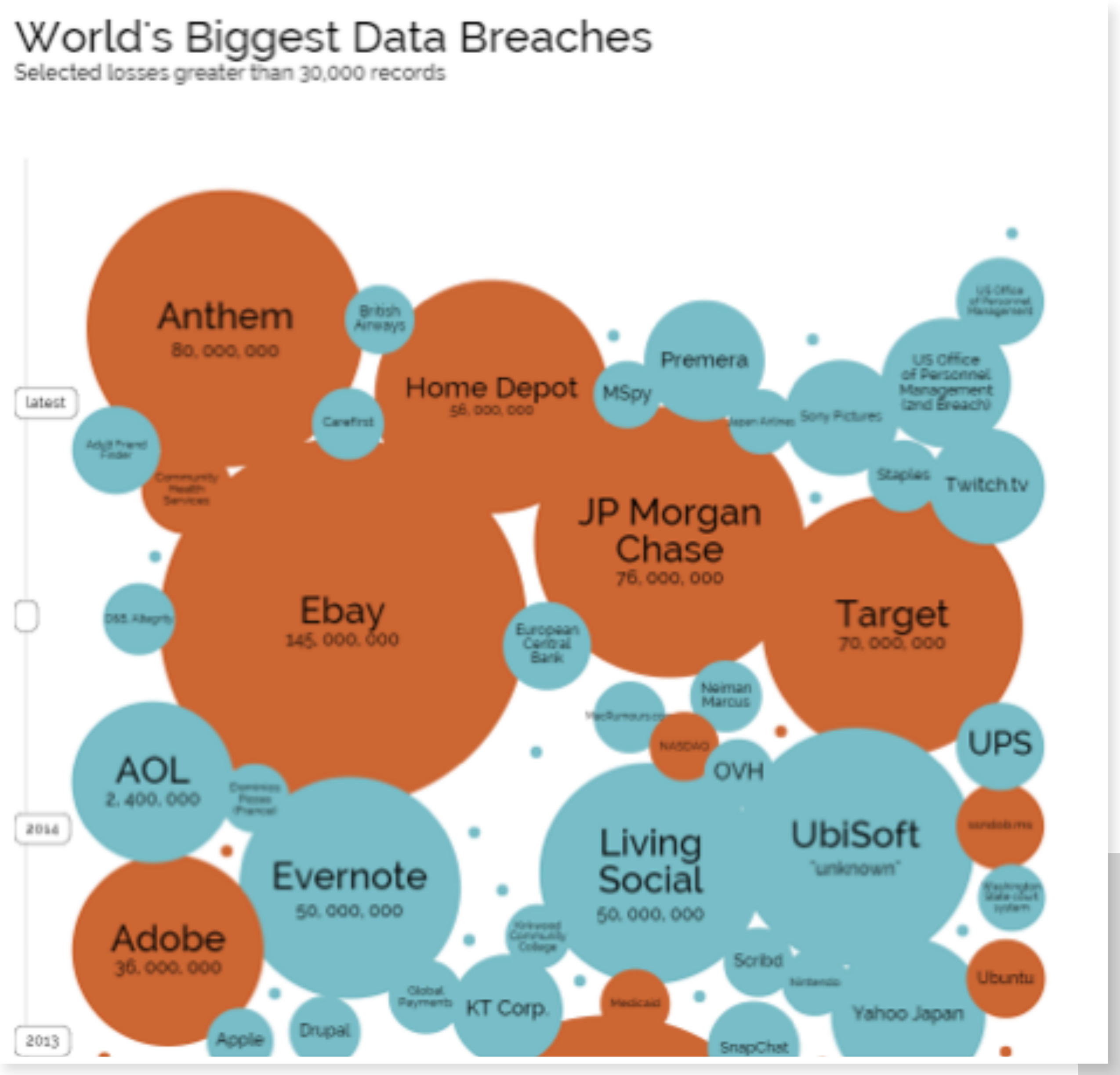
NetWatcher

Yet SMB's Are Not Prepared!

- 86% of businesses said they are "satisfied" with the level of security they have in place to defend customer or employee data
- 87% of respondents have not written a formal security policy for employees
- 83% lack any security blueprint at all
- 59% have no plan in place to respond to a security incident

– *National Cyber Security Alliance (NCSA) and Symantec "National Small Business" survey*

Everyone Is A Target…



World's Biggest Data Breaches

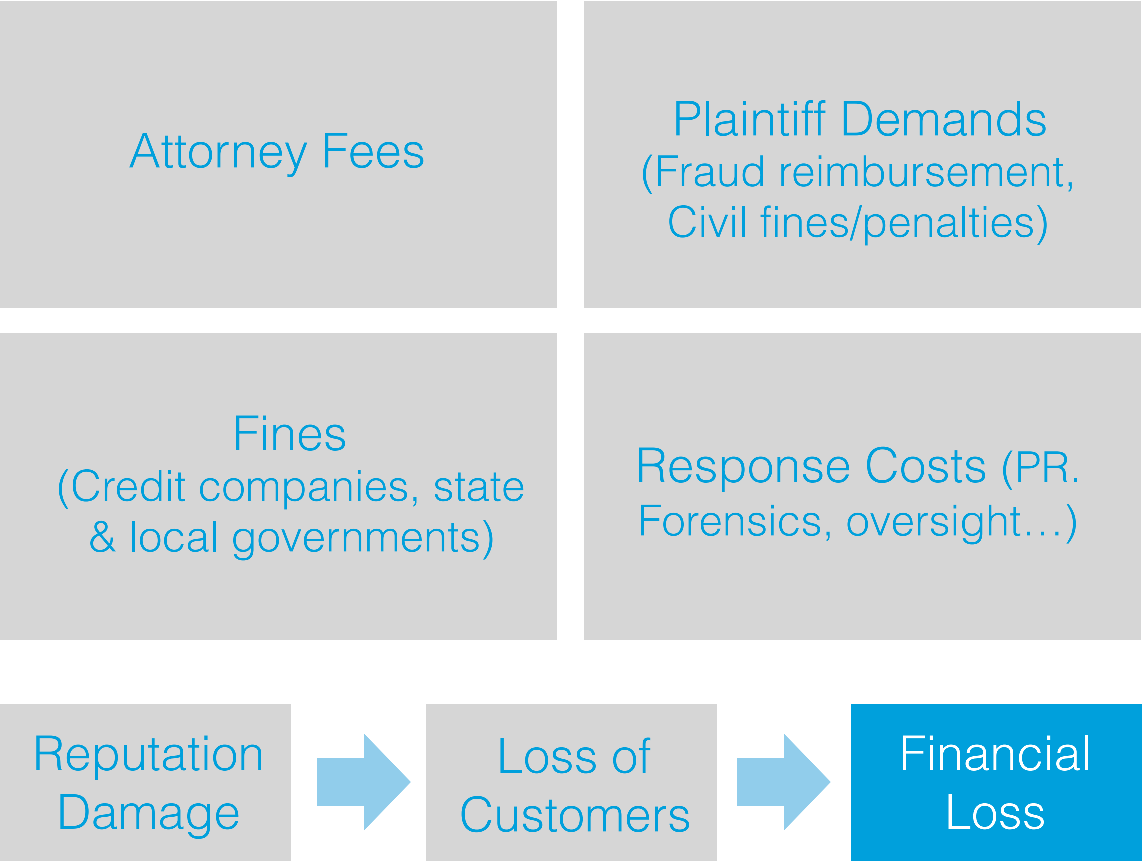
Selected losses greater than 30,000 records

http://www.databreaches.net/
https://www.privacyrights.org/data-breach
http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

NetWatcher

What Will A Breach Cost You?

A National Cyber Security Alliance study showed that 36 percent of cyber attacks are conducted against SMBs. Of those, up to 60 percent go out of business within six months of an attack.



Attorney Fees

Plaintiff Demands (Fraud reimbursement, Civil fines/penalties)

Fines (Credit companies, state & local governments)

Response Costs (PR. Forensics, oversight…)

Reputation Damage → Loss of Customers → Financial Loss

How Will You Be Attacked: Phishing

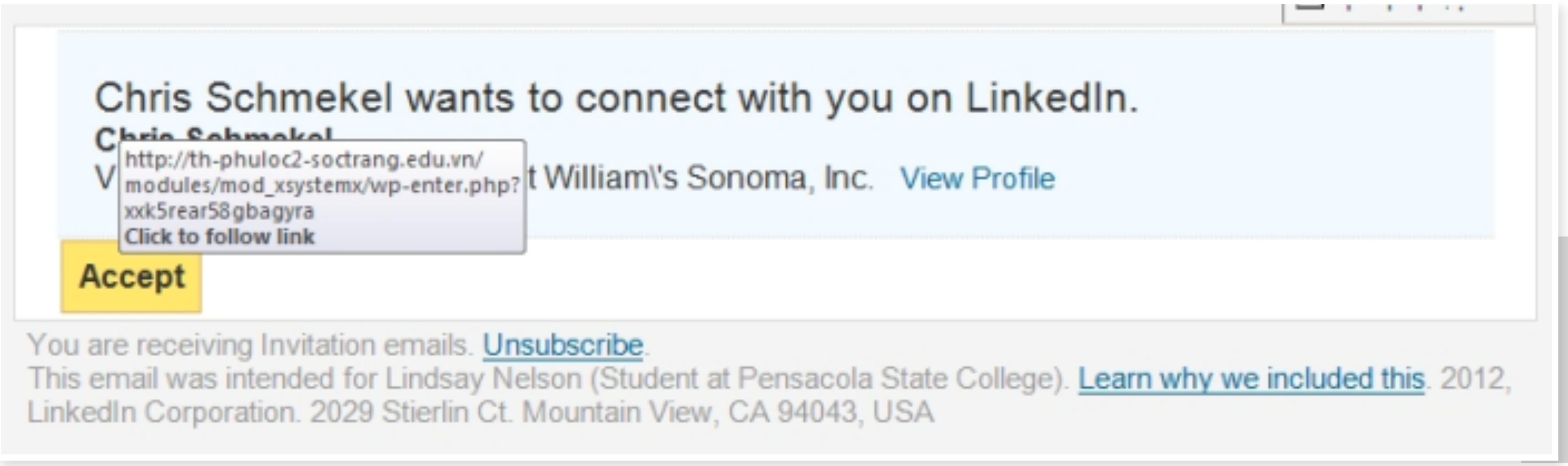
(Social Engineering) – The #1 Attack Vector!

You or one of your employees may receive a fake email or text message with a website created to look like it's from an authentic company.

What it does:

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Convince you to download Malware

39 Percent of Employees Admit to Opening Suspicious Emails



Chris Schmekel wants to connect with you on LinkedIn.

Chris Schmekel

V t William\'s Sonoma, Inc. View Profile

http://th-phuloc2-soctrang.edu.vn/modules/mod_xsystemx/wp-enter.php?xxk5rear58gbagyra

Click to follow link

Accept

You are receiving Invitation emails. Unsubscribe.

This email was intended for Lindsay Nelson (Student at Pensacola State College). Learn why we included this. 2012, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

NetWatcher

How Will You Be Attacked: Others…

Pharming

Cross Site Scripting

Denial of Service

SQL Injection

Dictionary Attack

Botnets

Scanning

***see appendix for details*

Your Employees Are Your Weakest Link…

You can have all the **Prevention** tools (Anti-Virus, Firewalls, Automatic Patching, Backups, Robust Password Protection etc..) and still be vulnerable to the introduction of code onto your network that can Sniff your traffic, Copy your data or Control your devices…

- Cyber Security --Your employees are your weakest link…
- Unmanaged BYOD and employees clicking on things they shouldn't are what let bad actors through the front door…

What You Must Do –

Cyber Liability Insurance

- Ensure you have the appropriate Cyber Insurance coverage for 1st party liability and possibly 3rd party liability
- Common first-party costs when a security failure or data breach occurs include:
  - Forensic investigation of the breach
  - Legal advice to determine your notification and regulatory obligations
  - Notification costs of communicating the breach
  - Offering credit monitoring to customers as a result
  - Public relations expenses
  - Loss of profits and extra expense during the time that your network is down (business interruption)
- Common third-party costs include:
  - Legal defense
  - Settlements, damages and judgments related to the breach
  - Liability to banks for re-issuing credit cards
  - Cost of responding to regulatory inquiries
  - Regulatory fines and penalties (including Payment Card Industry fines)
- Ensure your coverage covers remediation!
- Example

What You Must Do –

Create a Corporate Cyber Policy

General
- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Ethics Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Infrastructure
- Database Credentials Policy
- Technology Equipment Disposal Policy
- Information Logging Standard
- Lab Security Policy
- Server Security Policy
- Software Installation Policy
- Workstation Security (For FINRA) Policy
- Web application security policy

Examples:
- Sample Policy (here), SANS (here)

Network Security
- Acquisition Assessment Policy
- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard
- Third Party Access Policy
- What software can I run on the network? Can I run TOR? BitTorrent?
- Can I get my personal mail via my company laptop?
- Can I use Facebook on my company laptop? During work hours?
- Can I plug in a WIFI router on my desk?
- Can I connect my personal phone to the corporate WIFI?
- Can I visit Porn sites on my corporate laptop?

What You Must Do –

Ensure you and your board have answers to the following questions…

- Who is responsible for developing and maintaining our cross-functional approach to cybersecurity? To what extent are business leaders (as opposed to IT or risk executives) owning this issue?
- Which information assets are most critical, and what is the “value at stake” in the event of a breach?
- What promises—implicit or explicit—have we made to our customers and partners to protect their information?
- What roles do cybersecurity and trust play in our customer value proposition—and how do we take steps to keep data secure and support the end-to-end customer experience?
- How are we using technology, business processes, and other efforts to protect our critical information assets? How does our approach compare with that of our peers and best practices?
- Is our approach to security continuing to evolve, and are we changing our business processes accordingly?
- Are we managing our vendor and partner relationships to ensure the mutual protection of information?

What You Must Do –

Employee Training

- Training - Continually raise your staff and contractors awareness on cyber security best practices (email, web, phone, text etc…)
- Train Employees
  - Forensic investigation of the breach
  - To recognize an attack
  - On step-by-step instructions about what to do if they've witnessed a cyber incident
  - On your corporate cyber policies

See Appendix…

What You Must Do –

Your Suppliers

- Do your suppliers / partners / contractors have access to your network or Line of Business systems?
- Audit your suppliers / partners / contractors for their cyber liability insurance coverage, their corporate cyber policies and their infrastructure protection

Understand Regulatory/Policy Compliance for Your Industry

- PCI-DSS Service for Small to Medium Businesses
- FINRA Service for Small to Medium Businesses
- HIPAA Service for Small to Medium Businesses

Big Fines…

What You Must Do –

Technology

- Systems
  - Forensic investigation of the breach
  - Ensure your computer systems' and security software stay up to date
    - Especially Java, Flash and Windows security updates
  - Secure & Encrypt laptops and mobile phones
  - Ensure Backup are scheduled and tested
  - Firewalls, latest routers/switches with up to date software

- Move your Line of Business systems to secure cloud providers:
  - Offsite cloud providers will require more stringent firewalls, access credentials and security protocols than onsite stored data.
  - Offsite cloud applications are stored within the walls of a 24/7/365 physically secured data center facility.
  - Cloud application providers build threat assessment models that will work to identify possible leaks within business cloud applications, and constantly work to break those security measures, in an effort to make them stronger and stronger.

- Software you have built
  - Needs to be secure by design (here)

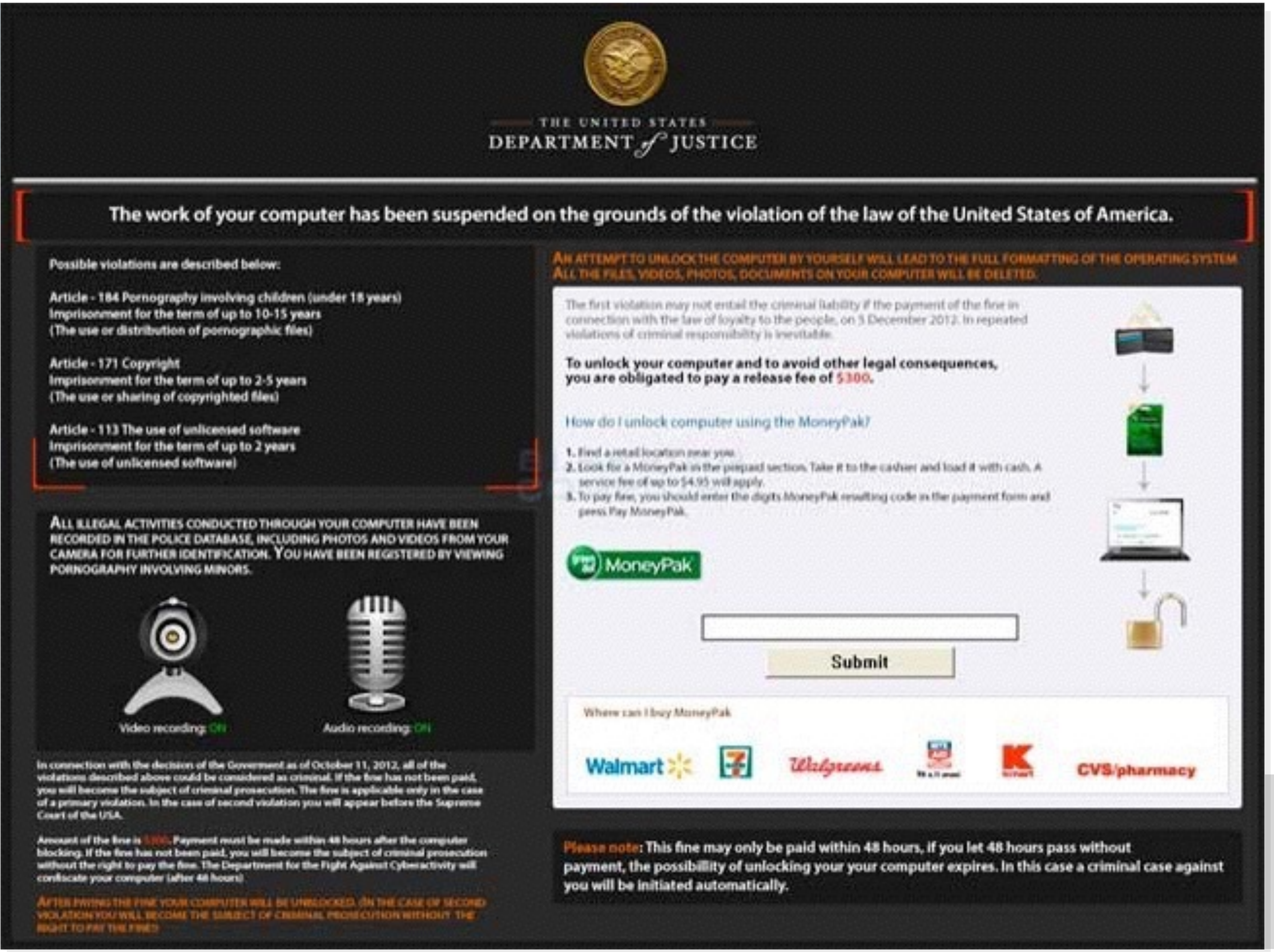
What You Must Do –

Technology

- Use a Managed Cyber Security Services like Defensative's NetWatcher™ services to continuously monitor your network for security threats and vulnerabilities
  - http://defensative.com

- Consider end-point technology from companies like http://triumphant.com
  - Triumfant integrates seamlessly into Defensative's NetWacher service.

Appendix



THE UNITED STATES
DEPARTMENT of JUSTICE

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article - 184 Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article - 171 Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article - 113 The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

Video recording: ON

Audio recording: ON

In connection with the decision of the Government as of October 11, 2012, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the Supreme Court of the USA.

Amount of the fine is $300. Payment must be made within 48 hours after the computer blocking. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer (after 48 hours)

AFTER PAYING THE FINE YOUR COMPUTER WILL BE UNBLOCKED. (IN THE CASE OF SECOND VIOLATION YOU WILL BECOME THE SUBJECT OF CRIMINAL PROSECUTION WITHOUT THE RIGHT TO PAY THE FINE!)

AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF THE OPERATING SYSTEM
ALL THE FILES, VIDEOS, PHOTOS, DOCUMENTS ON YOUR COMPUTER WILL BE DELETED.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people, on 5 December 2012. In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

Where can I buy MoneyPak

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your your computer expires. In this case a criminal case against you will be initiated automatically.

How Will You Be Attacked:

Pharming

You or one of your employees may be pointed to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.

What It Can Do:

- Convince you that the site is real and legitimate by looking almost identical to the actual site down to the smallest details. You may even enter your personal information and unknowingly give it to someone with malicious intent.
- Convince you to download Malware.

How Will You Be Attacked:

Cross Site Scripting (XSS)

You or one of your employees opens a website that has embed hidden scripts, mainly in the web content, to steal information such as cookies and the information within the cookie (e.g. passwords, billing info).

How Will You Be Attacked:

Denial of Service (DOS)

A bad actor will attempt to make one of your network resources unavailable to its intended users by saturating the target with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

How Will You Be Attacked:

SQL Injection

A bad actor may try to get valuable information from your website by exploiting vulnerabilities in the sites databases.

How Will You Be Attacked:

Dictionary Attack

A brute force attempt to guess your network assets passwords, by using common words and letter combinations, such as “Password” or “abc123”.

How Will You Be Attacked:

Botnets

A collection of software robots, or 'bots', that creates an army of infected computers (known as ‘zombies') that are remotely controlled by the originator. Yours may be one of them and you may not even know it.

<u>What They Can Do</u>:

- Send emails on your behalf
- Spread all types of malware
- Can use your computer as part of a denial of service attack against other systems

How Will You Be Attacked:

Scanning

Your hosts are being scanned daily by server farms all over the world looking for current vulnerabilities (example: Heartbleed) that you may not have patched yet…

What They Can Do:

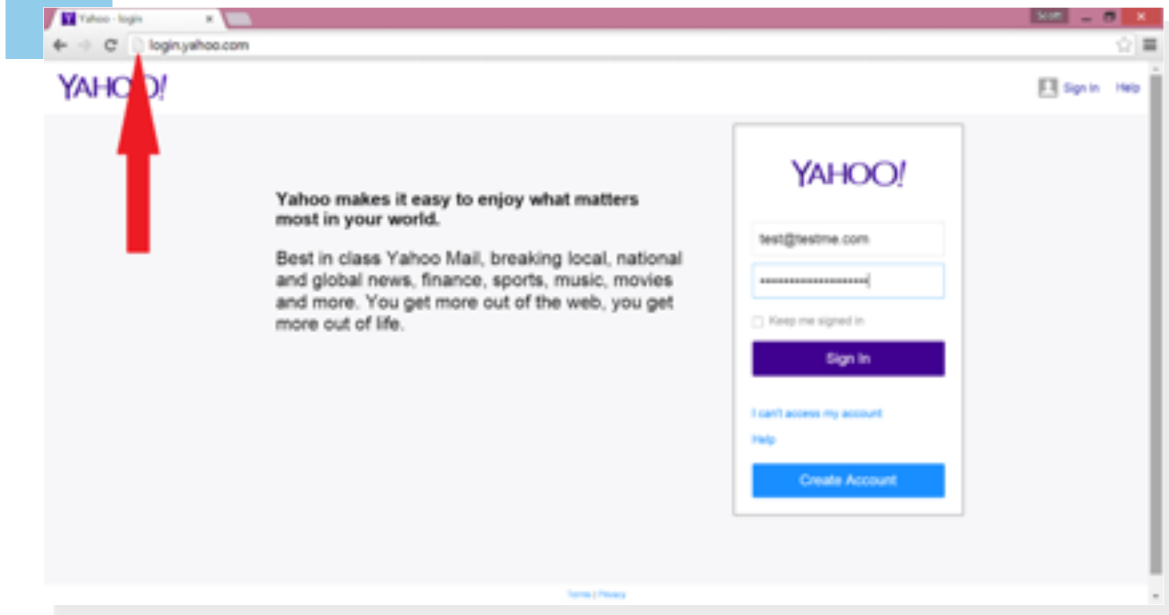
- Take control of your company…

Slides from End User Training

What You Must Do

Use HTTPS

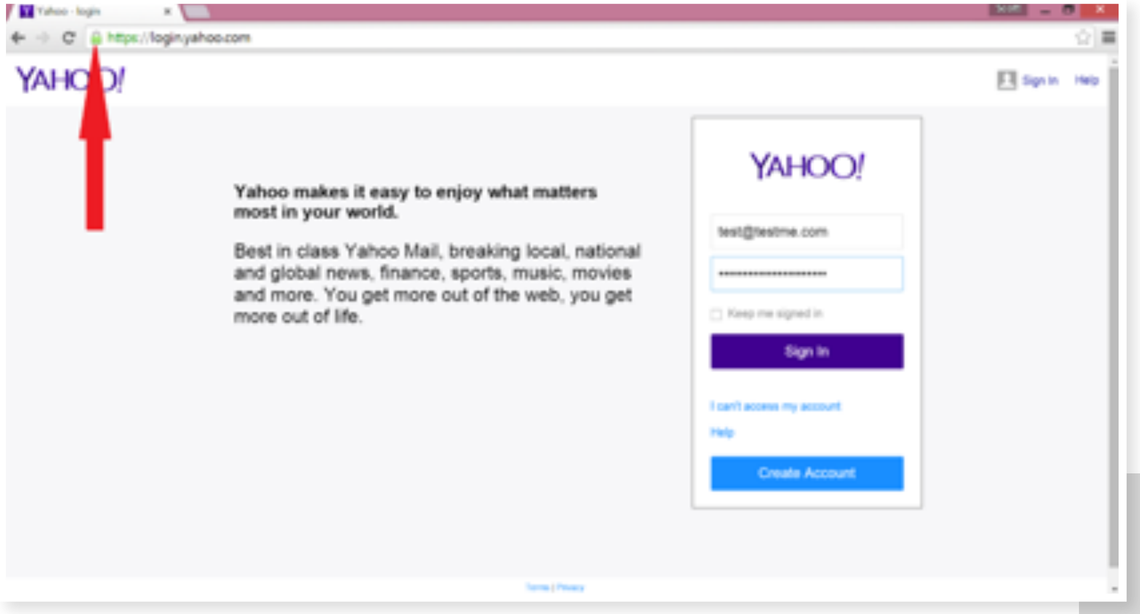
Unfortunately many websites and services today still offer un-encrypted login. With un-encrypted login, the password is NOT encrypted and considered "cleartext" and can be easily decoded!


login.yahoo.com

Yahoo makes it easy to enjoy what matters most in your world.

Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

test@testme.com


https://login.yahoo.com

Yahoo makes it easy to enjoy what matters most in your world.

Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

test@testme.com

More here, and here

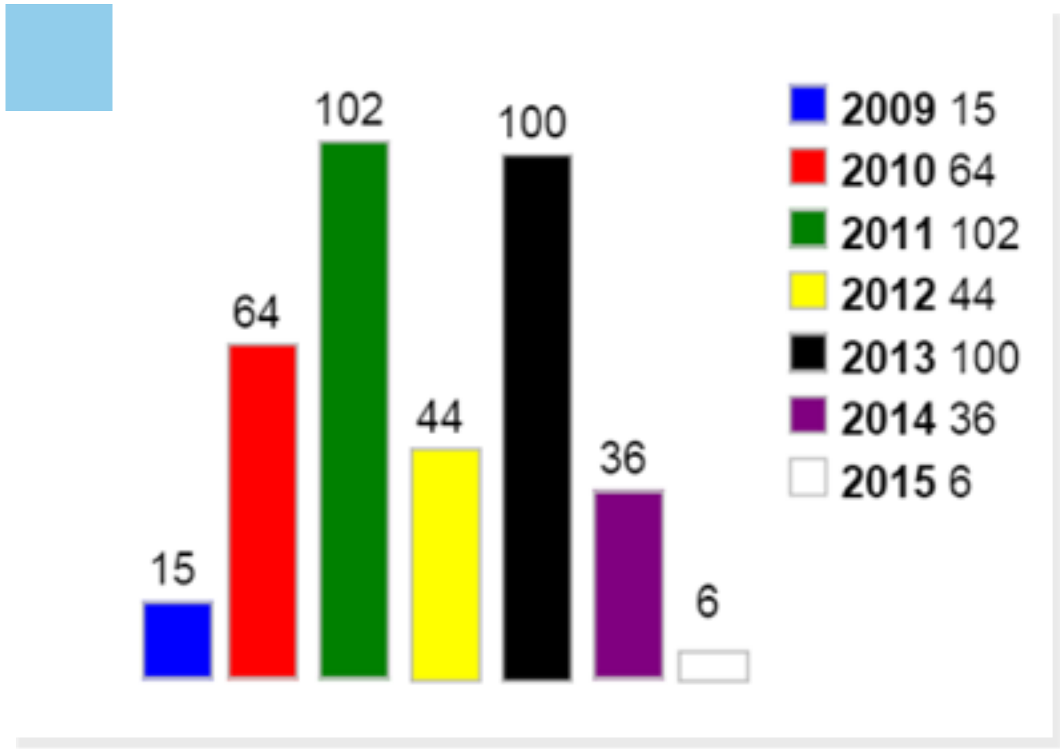
What You Must Do

Keep Software Up-to-Date

Software vendors such as Adobe, Microsoft, Oracle and others produce frequent security patches that plug holes that can be exploited by bad actors.

If you don't install these patches on a regular basis on your hosts, desktops, laptops and phones your infrastructure will be at risk and will eventually be compromised.

CVE Details is a good place to keep up on the patches. They consolidate vulnerability data from the National Vulnerability Database (NVD) and www.exploit-db.com . Another great site is Mitre's CVE site here .



Here are 2 examples to give you some perspective on how many vulnerabilities a software can contain:

- Here is a list of Adobe Flash vulnerabilities.
- Here is a list of Oracle Java vulnerabilities.
- Here is a simple chart that shows how many vulnerabilities have been published over the years in the Windows 7 OS

NetWatcher

What You Must Do

Don’t Use Risky Software

Examples:

- BitTorrent - you have no control over what the BitTorrent user is downloading and you don't want to end up like this guy . (or these people)
- TOR – You don’t know who is sniffing on the exit nodes (example)
- TFTP – It’s all in clear text (more)
- Misc Android Apps – 97% of mobile malware is on Android (more) (example)

What You Must Do

Passwords

- Use Secure Passwords (more)
- Use throw away passwords on non-mission critical sites
- Understand Password Managers may not be that secure (example)
- Change Default Passwords! (more)
- If available enable two factor authentication (example)

What You Must Do

Your Phone

Here are 7 Tips to Prevent Mobile Malware:

- Understand the mobile risks - A mobile device is a computer and should be protected like one. If you access the corporate network with their mobile device you should understand the risk imposed by downloading applications and accessing website that are not from trusted sources. You need to also know the value of keeping your operating system on the device up to date with the latest security patches from the manufacturer/mobile provider and operating system vendor.
- Only access corporate data via Wi-Fi over a secure tunnel as over the air networks are exposed to malicious capturing of wireless traffic. There are several mobile Virtual Private Networking technologies (VPN) that can be deployed that can allow users to connect through these secure tunnels.
- Understand your companies Bring Your Own Device to work (BYOD) policies
- Ask your company if they have a Mobile Device Management (MDM) platform and Mobile Application Management Platforms from companies like Good and others.
- Encrypt your devices - It is very difficult for someone to break in a steal data on an encrypted device (this goes for the SIM card as well).
- If you use Android then use anti-malware software

What You Must Do

Home Networks & Public WiFi's…

- Change the default password and keep the firmware up to date on your home internet router
- Don't connect to random WIFI's (example)
- Don't allow others to download programs to computers or phones that will connect to your companies network. Here is a Minecraft example.
- Use a Virtual Private Network (VPN) (example, example)

What You Must Do

Explicit Sites

Pornography and Malware… They go together. (more)

Visitors to Pornhub.com, the 63rd most popular website in the world (and 41st in the US) have a 53% chance of coming into contact with malware

What You Must Do

Know What You Should Do if You Suspect You Have Been Compromised

Great Advice from SecurityMetrics (here)

- Disconnect from the Internet by pulling the network cable from the router to stop the bleeding of data. Do not turn off your computer/phone/tablet
- Follow your company cyber security policy step by step plan. The company will usually:
  - Document all network changes, notification/detection dates, and people/agencies involved in the breach
  - Segregate all hardware devices in the payment process, or devices suspected of being compromised (if possible) from other business critical devices.
  - Quarantine instead of deleting.
  - Preserve firewall settings and firewall logs
  - Restrict Internet traffic to only business critical servers and ports outside of the credit card processing environment.
  - Disable (do not delete) remote access capability and wireless access points.
  - Call a PFI. Once the breach is contained by steps 1-7, consult with a forensic PFI to plan a compromise analysis.