

Truths & Myths About Hackers, Malware & Computer Security

Cybersecurity 101 for Government Agencies and Contractors





- Fact -

NASCIO - State CIO Priorities for 2016



- Myth -

Cyber threats are not
increasing in complexity
and intensity



- Fact -

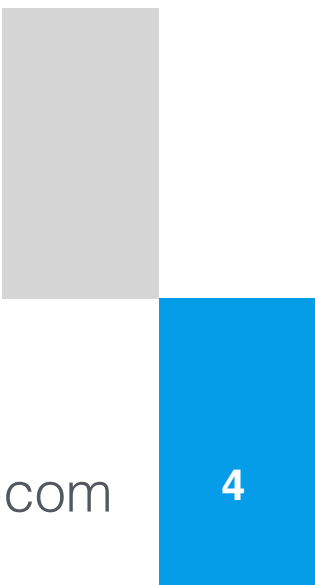
Funding for
cybersecurity
initiatives is insufficient





- Myth -

For a small company,
security talent is easy
to find and not very
expensive.





- Fact -

There is a significant
lack of cybersecurity
visibility and control



- Myth -

Smaller agencies and
SMB's have NOT
become the new target

What Are They After?

- Money – [Ransom-ware](#)
- Your organization'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 customers/partner' data & access to your customers networks...
 - The Target breach happened due to an HVAC vendor

Are You Prepared?

- If you are anything like the typical small or medium sized enterprise then no, you're not fully prepared.
 - 86% of SMB's said they are "satisfied" with the level of security they have in place to defend customer or employee data
 - 87% of SMB's 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



A Breach Will Cost You Money

1. Attorney Fees
2. Plaintiff Demands
3. Response Costs
4. Reputation Damage

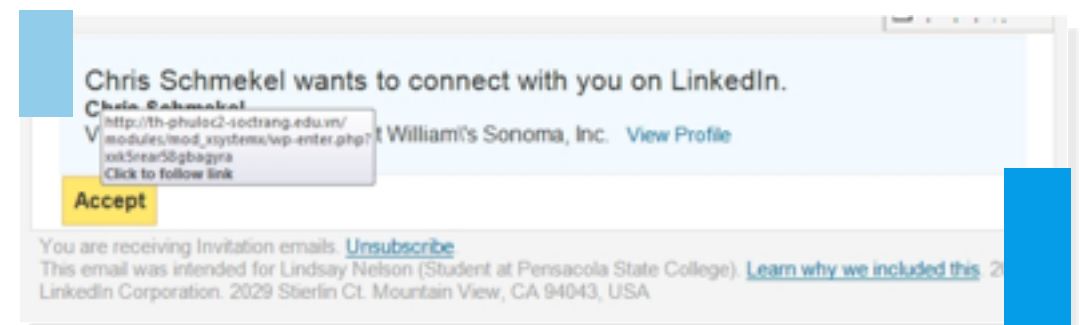
Your Employees Are Your Biggest Risk

They are 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



Many Ways To Take You Down

1. Pharming
2. Cross Site Scripting
3. Denial of Service
4. SQL Injection
5. Dictionary Attack
6. Botnets
7. Scanning



- Myth -

Proper cybersecurity
is expensive



- Fact -

Security is less about
technology and more
about business process



Cyber Liability Insurance

What you must do

- Ensure you have the appropriate Cyber Insurance coverage for both 1st party liability and 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)

Cyber Liability Insurance

What you must do

- 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!

Create IT & Employee Policies

What you must do

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

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

Create IT & Employee Policies

What you must do

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

Make This a Leadership Problem

What you must do

- Who is responsible for developing and maintaining our cross-functional approach to cybersecurity? To what extent is leadership (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? – Focus limited resources on protecting these assets!
- Understand what promises—implicit or explicit—have you made to our customers and partners to protect their information?

Make This a Leadership Problem

What you must do

- What roles do cybersecurity and trust play in your customer value proposition—and how do you take steps to keep data secure and support the end-to-end customer experience?
- Compare your approach with your peers.
- Is your approach to security continuing to evolve, and are you changing your business processes accordingly?

Manage Your Suppliers

What you must do

- 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
 - Make this a part of their contract!



Routine Audit

What you must do

- Create a process for periodic audits

Have A Response Plan

What you must do

- Create a cross-organization response plan
 - Practice
 - Train everyone

Understand & Leverage Technology

What you must do

- 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 (and no default passwords)
- Engage a Managed Security Services Provider (MSSP) like IH Solutions who offers an end-to-end platform such as NetWatcher rather than buying expensive solutions like FireEye.

Understand & Leverage Technology

What you must do

- 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

Conduct “Everyone” Cyber Training

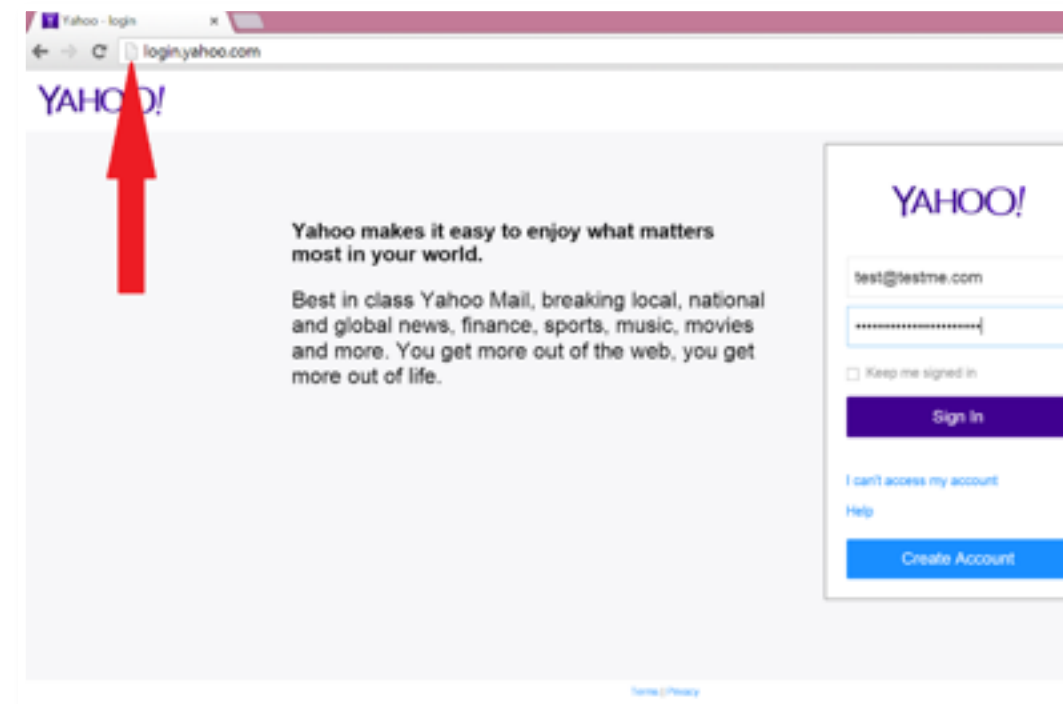
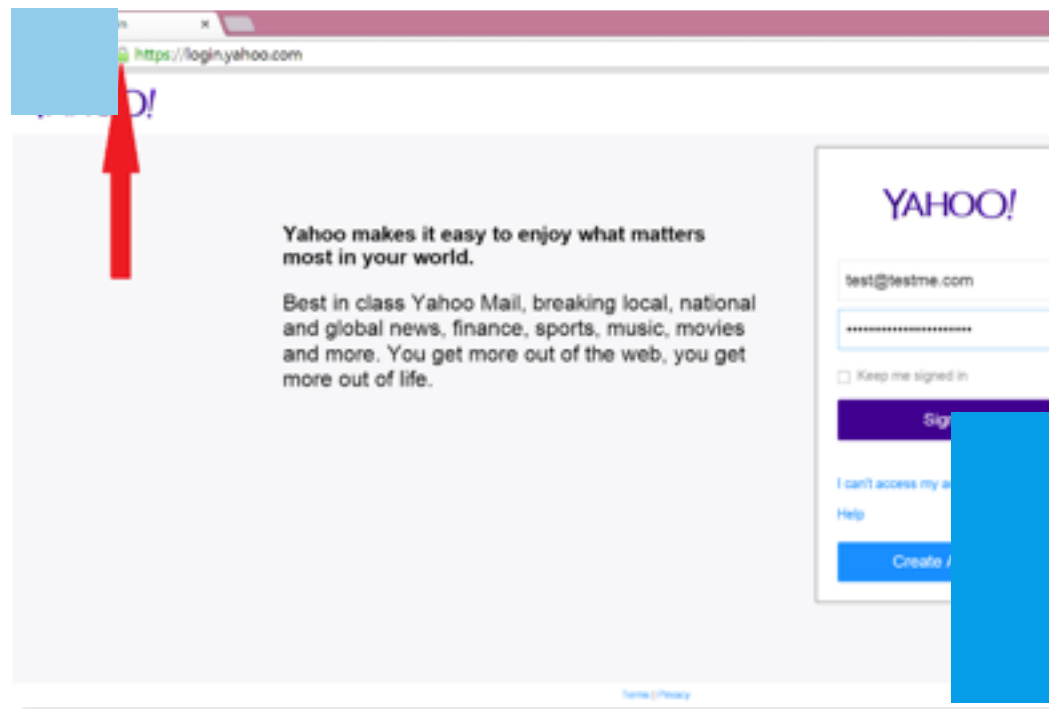
What you must do

- Training - Continually raise your staff and contractors awareness on cyber security best practices (email, web, phone, text etc...)
- Train employees
 - 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

Use HTTPS, Not HTTP

Train Employees

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!



Keep Software Up to Date

Train Employees

- 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.

Keep Software Up to Date

Train Employees

- 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

Don't Use Risky Software

Train Employees

- 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](#))

Use Secure Password

Train Employees

- 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](#))

Prevent Mobile Malware

Train Employees

- 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.

Prevent Mobile Malware

Train Employees

- Understand your group's [Bring Your Own Device](#) to work (BYOD) policies
- Ask your organization 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

Home Network & Public Wifi

Train Employees

- 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](#))

Explicit Sites

Train Employees

- Pornography and Malware. They go together.
 - 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

Know What To Do

Train Employees

- 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 groups cyber security policy step by step plan. Your group 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.

Know What To Do

Train Employees

- Follow your groups cyber security policy step by step plan. Your group will usually:
 - 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.

Appendix

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.



Cross Site Scripting

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 (eg passwords, billing info).



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.



SQL Injection

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



Dictionary Attack

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



BotNet Attack

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.

What They Can Do

- 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



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 organization.