SAFE CYBER HYGIENE FOR WORK AND AT HOME

NJ Government Records Council
Annual Training Seminar
August 10, 2017
By Marc Pfeiffer, Assistant Director
Bloustein Local Government Research Center
Rutgers University

FIRE IN OHIO SCHOOL
TEXAS CITY EMPLOYEES HACKED

- SERVERS SUSCEPTIBLE TO HACKERS IN BASEMENT OF WRECKED BUILDING
- W-2 FORMS OF 800 CITY EMPLOYEES FALL INTO HANDS OF SCAMMERS
BOTTOM LINE

- Criminals try to manipulate people into divulging personal or business information or trick them into schemes to defraud
- Criminals can be individuals or part of industrialized, cyber crime businesses

No single fix since the threats keep changing; It’s a perpetual battle
Some Common Terms

Malware

Destructive form of computer software transmitted by email and website links
Phishing
a form of social engineering that appears as email or a text message that attackers use to gain login credentials or account information

And its evil cousin, the targeted **Spear-Phish** or **Vish**, using voice to fool you

**WHY SHOULD I CARE?**

- **60%** of employees will click a phishing link
- **30%** of them will actually give up organization credentials
- **20%** stated they would sell their organizational password

**REALITY:** the bulk of successful attacks come because an employee clicked on something they shouldn’t have
Types of Attacks and Threats

• **Targeted Attacks**
  – Government agencies are generally targets
  – It also happens if something goes wrong

• **Mass Attacks**
  – This stems from successful email phishing, social engineering, plus “brute force” attacks on networks

• **Man-in-the-Middle Attack:**
  – A link to a log-in site that looks legit, but is fraudulent and will steal your credentials

• **Unsecure humans**
  – Clicking on the wrong link/opening the wrong file
  – An employee who steals data for resale or illegal use
PHISHING EMAILS EXAMPLES

Phishing email poses as an important email from a trusted organization

- A notification from the post office, UPS, FedEx shipping informing the recipient of a delivery
- A message from a utility provider or retailer about an overdue bill
- An alert about the recipient’s tax return
- Invoices or notices for goods and services (Amazon, Costco)
- Fake credit card reward schemes
- Direction from your employer, i.e., need to log-in because you lost some permission

Each variation relies on our instinct to act on messages that appear to be urgent.

TOP FIVE CEO WIRE FRAUD ATTACKS

FBI: $2.3 Billion in BEC* Losses

- **270%** Increase in Business Email Compromise (BEC) attacks reported by the FBI from Jan. 2015 through Mar. 2016
- **14,000+** Number of victims the FBI reports who have reported BEC attacks
- **11%** Number of U.S. companies that say attackers have sent them a wire fraud email**

How CEO Email Wire Fraud Works

- Attacker Posing as CEO
- Specified Wire Funds Request
- Finance Employee
- Wire Transfer
- Company’s Bank Account
EMAIL AS SOURCE OF MALWARE?

- Embedded, but fake links entice you to open harmful websites
- Spoofed “from” addresses
- Attachments that are or have embedded viruses or malware (docx, xlsx, pptx, html, zip)
  - MS Office documents can have malicious macros in them
- Embedded images containing hidden code exposing you to harm
- Coupons and advertisements with “hidden agendas”
REASONS FOR CLICKING?

- CURIOSITY = 34%
- MET AN EXPECTATION = 27%
- INVESTIGATION = 17%
- KNOWN SENDER = 16%
- TRUST IN CONTEXT = 11%
- FEAR = 7%
- AUTOMATIC = 3%

• Clicking on an attachment or a link embedded in a suspicious email launches a program that encrypts (or rewrites) your files
SO WHAT HAPPENS?

• The files are held for ransom; the hacker who sent the email will require a payment from you before they will (hopefully) send you the **key** (a line of computer code) that decrypts the files and restore them.

• Hope you have backups to restore your system; otherwise you pay!

• Now known to hackers as a victim and will be subject to future attacks
WHEN EMAIL TURNS EVIL

Someone has your password

Google <no-reply@accounts.googlemail.com>
to me

12:02 (1 hour ago)

Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 10 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD
PROTECT YOURSELF FROM EVIL EMAIL

- Learn to hover and read links!
- Be suspicious of unexpected emails
- Do not open attachments you are not expecting:
  - Confirm first with the sender if it looks important
  - Or just delete it
- Always be suspicious (do not let your guard down)
- If it doesn’t look right, it’s not right
- Do not log in to an account from an email link unless you verify it’s a legit email and site
- Never unsubscribe from a group that you are unfamiliar with or did not subscribe to
“But, I Think I’m Smart About This”

• “I knew, if this was something dangerous, my Norton would protect me”
• “I use Firefox and MacOS, so I’m not afraid of the viruses”
• “After I googled it, Photocloud.com seemed to be a clean website”
• “I googled the email address [...] I found nothing”
• “I consider our webmail to be safe”
HOW STRONG IS YOUR PASSWORD?

- A six character, single case password = **308 million** possible combinations
- Combining upper and lower case and using 8 characters instead of 6 = **53 trillion**
- Substituting a number for one of the letters yields **218 trillion**.
- Substituting a special character **6,095 trillion**.

What That Means to You

- Use strong passwords or better **yet pass-phrases**, do not use names, date of births, or anything known about you
- Change them periodically
- Do not share passwords! But, if you must consider that:
  - Anything that happens on that account gets treated as if you did it
  - If you do share a password, change it to something generic before and back to something complex after; or change it after it’s use
- **Use a personal password manager**
SAFE WEB BROWSING

A password is like a toothbrush

Choose a good one

Don't share it with anyone

Change it occasionally

The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place

© Bloustein Local Government Research Center, Rutgers University
THE PROBLEMS WITH BROWSING

- Use of passwords on insecure pages
- Malware loaded pages
- Unexpected pop-ups

This is not your mother’s internet!
If you are unsure about this type of pop-up, search for “flash update” and go to an adobe.com site to check. Don’t download from a pop-up that’s not from the adobe.com website.
Beware of free downloads from coupon and download sites – malware often follows!
And watch where you click!
Your Mac OS may have Porn Virus!

OS Version: OS X 10.12
Location: South Bound Brook
IP Address: 148.76.54.124
ISP: Optimum Online

These harmful viruses may damage your device's system files and all your existing contacts might be lost.

Click “Remove Now” to download MacKeeper and run a full system scan immediately!

Your Mac OS may have Porn Virus!
These harmful viruses may damage your device’s system files and all your existing contacts might be lost.

Pending. Please uncheck elements you don’t want to remove.

All programs will be closed in order to proceed correctly to the removal of the infections. Please save any work in progress and then click [OK].
Safe Browsing @Work and @Home

• **DO NOT CLICK ON** suspicious pop-ups or unexpected messages when browsing!
  – If at work, call IT; if at home, close the window or, disconnect from network
  – Work is work, not home!
  – Remember your web browsing activities are tracked (even if you clear the browser history)!
  – **DON’T CLICK** on that pop-up!
  – Test a page by looking at it full size and then shrinking it. If it won’t or doesn’t, close the browser!

• **DON’T CALL** the number on the screen
• Things that are too good to be true, aren’t true. Don’t click on them or delete them
• Caught in a loop? Shutdown and reboot
• **Stay Safe**: Browse trusted sites:
  • Know the address: HTTP vs. HTTPS, and no passwords on non-https sites
  • Use two-factor authentication when offered
  • Don’t download “tool bars” or cleaners, unless known or checked out. You probably don’t need them

**KEEP YOUR COMPUTER UP TO DATE**
Keep windows, antivirus, and browser updated with latest versions
Forms of Social Engineering

- In-person
- Phone
- Digital

Hard Drive Safety Delete Starting In 4:26

To STOP Deleting Hard Drive Call: 1-866-359-6475

ERROR CODE: 0x000314CE

Please contact technical support Toll Free: 1-866-359-6475
To immediately rectify issue and prevent data loss
BEWARE OF...

...phone callers asking for confidential employer or personal information, even if they claim to be from IT or a vendor. Refer them to IT support or hang up.

'Can you hear me?' phone scam
Faux telemarketers asking unwilling victims to respond with a single word to "Can you hear me?"
Do not reply with "yes"

Don’t clink on text message links from someone you don’t know

USB SECURITY

- 48% of people plug in USB drives found in parking lots

Dropping USB Sticks is Effective

People plug in USB drives quickly
UNFORGETTABLES

• Do not log on and off a computer when asked by another employee or outside person – unless identity is verified
• Caller ID can be “spoofed”
• Use two-factor authentication transactions whenever it's available
• Fiscal and HR people: POSTIVELY confirm all emailed directions for anything (especially for personnel information and payment direction)
• Use passcode on mobile devices
**UH, NOPE**

- No system is 100% perfect - since threats are always changing
- Stay aware: stop, think, then connect
- Call your IT support person when in doubt
- At home: [www.malwarebytes.org](http://www.malwarebytes.org) if you get infected

---

**PUTTING IT ALL TOGETHER**

- Don’t be curious – just don’t click
- Online; free is never free
- Be suspicious – hover first and check it out
- If you didn’t ask for it, you don’t need it
- **Never** open attachments from unknown people
- **Don’t instinctively** open files from people you know but were not expecting; check with them first
- Lock your PC when away from your desk
  - “Ctrl + Alt + Del > Enter” or “Windows + L”
- Test yourself: search for **“Pew Cybersecurity Quiz”**
  - [www.pewinternet.org/quiz/cybersecurity-knowledge/](http://www.pewinternet.org/quiz/cybersecurity-knowledge/)
YOU KNOW WHAT THEY SAY...

CURIOSITY KILLED THE CAT

KEEP CALM
AND
STAY CYBER SAFE

For more information for work or home or school:
www.stopthinkconnect.org
FOR FURTHER DISCUSSION & COMMENTS

Marc Pfeiffer, Assistant Director
Bloustein Local Government Research Center
Bloustein School of Planning and Public Policy
Rutgers University
Marc.Pfeiffer@rutgers.edu

- Technology Risk Management Papers at:
  - [http://blousteinlocal.rutgers.edu/managing-technology-risk/](http://blousteinlocal.rutgers.edu/managing-technology-risk/)
- Or search for “Bloustein Technology Risk”

AND NOW...
SOME WORDS ABOUT TECHNOLOGY RISKS AND PROFICIENCY
Categories of Technology Risk

- Cybersecurity
- Financial
- Operational
- Legal
- Societal
- Reputational

THREE ELEMENTS OF PROFICIENCY

Technology Management
- Governance - decisions
- Planning – what to do
- Budgeting – how to fund

Cyber Hygiene
- Employee training
- Adopted policies
- Encryption of PII and PHI

Technical Competency
- Meets minimum standards
- Access to expertise
- Incident response plans
MINIMUM ACCEPTABLE LEVELS:
TECHNICAL COMPETENCY

- Minimum Backup Practices
- Server Physical Security
- Timely Software Patching
- Access Privilege Controls
- Strong Defensive Software
- Technology Support

MINIMUM ACCEPTABLE LEVEL:
SOUND CYBER HYGIENE

- Employee training
- Policies: Email, Internet, Password
- Protect PII and PHI
- Password strength

© Bloustein Local Government Research Center, Rutgers University
MINIMUM ACCEPTABLE LEVEL: TECHNOLOGY MANAGEMENT

- Leadership has access to tech expertise
- Incident response plans