Effective Security Awareness Training for Law Firm Personnel

Presenters: Sharon Nelson and Jody Westby
Training Training Training
Have We Mentioned Training?

Don’t be stupid!
“The adage is true that the security systems have to win every time, the attacker only has to win once” – Justin Dykes, CISSP

- Technology is 10% of the solution, employees are 90%.
- January/February 2018 edition of Infosecurity Professional
Three Aspects of Cybersecurity Training

- Policies and Procedures
- People
- Technology
The policy side of security

- Policies and procedures define operations and employee actions
- Enforcement of policies is essential
- Security awareness training must be in policies
- Completion of training should be a factor in performance reviews
The people side of security

- Focus of training is on employee actions
- Securing data is everyone’s job
- Technology can help, but security is everyone’s responsibility
- People have to know what to do and what not to do...and when to report things
The tech side of security

- Technology helps achieve security
- Securing data with technology offers some solutions
- Enterprise level security software (e.g. Proofpoint, Mimecast, etc.) protects you from malware, spam, phishing but . . .
- There is no silver bullet!
Training tips for employers

- Options: formal training, online modules, random alerts / electronic postings
- When to formally train? Lunch is the most popular; one hour good timeframe
- Make training mandatory – sign-in sheets and logs
- Forbid the use of smartphones or other devices – and phones silenced
- Outside trainers – not your in-house IT
- Live is preferable but not always possible
- Real-life stories/phishing examples
- Train annually (at least!)
Videos – Sophos 1 minute security videos
Having set the stage, let the training begin!
SECURITY POLICY
Policies are foundation for culture of cybersecurity
Obey all security-related policies of your firm!

- Policies and Procedures: Information Security and Operational

- Acceptable Use Policy very important but not the only one.

- Enforcement can include disciplinary action up to and including termination
77% of users ignore social media policies (Oct. 2016 PewResearch Center)
Piggybacking

- Person enters building – or office – with you (tags along)
- Consent of the authorized user
- Appears to have authorization to be there
- The infamous Virginia office “creeper”
Tailgating

- Someone smoking or talking on phone near door catches the door you’ve opened using your key/prox card/biometrics etc.
- Follows authorized person without consent
- Human nature – we don’t challenge authority
Sharing credentials – what are you thinking?

- Do you have ABSOLUTE trust?
- If one gets breached, both are breached
- Policies should forbid sharing log-in credentials
"The user's going to pick dancing pigs over security every time."

Bruce Schneier
INTERNET SCAM!

IF IT SOUNDS TOO GOOD TO BE TRUE
THEN IT PROBABLY IS!
Phony Facebook coupons

- Click on coupon, go to site with malware on it
- Take a survey first (never get coupon) and give scammers your personal data
- They sell data to advertisers (or criminals) to target you with ads
- Share the coupon and get your friends in the same trouble
Phony Facebook coupons

Home Depot is giving $50 coupons for EVERYONE! to celebrate Mother's Day!
Get yours here - (1 Coupon) per person
HOMEDEPOT.COM-WEEKLYADS.US
Phony Facebook coupons
Social engineering

- 1 in 3 employees will fall for this
- Microsoft tech support
- Call from your IT company
Easy to be fooled....

- Phishing, especially spear phishing – most successful way of breaching law firms – an e-mail from a friend/colleague can be spoofed. Hackers research personal details too – may know nickname
91% of hacking attacks begin with a phishing e-mail

- 2016 PhishMe study
- Why do users click?
  - Curiosity (racy New Year’s photos)
  - Fear (bar complaint attached)
  - Urgency (boss needs this today)
  - Recognition (award you’ve gotten)
- SonicWall, Duo Security and OpenDNS
- One phishing simulation (reported to employees) drops risk of phishing success by 20%
Always check for spelling errors
Most successful phishing templates click rates

- 2018 “State of the Phish” report from Wombat Security
- Online shopping security updates – 86%
- Corporate voicemail from unknown caller – 86%
- Corporate e-mail improvements – 89%
- Database password reset alert – near 100%
- Updated building evacuation plan – near 100%
Business e-mail compromises

- FBI - $5 billion raked in 2013-2016
- Instructions to wire money, send check or send employee W-2s (to file phony returns with refunds)
- Thieves spoof e-mails and have insider knowledge of employer, employees, clients – and cases
- BEC may be preceded by phishing e-mail to get more info
Whaling

- Pretending to be a high level executive
- Real case – sent invoices to client who paid roughly $277,000 to the account specified in e-mail
- Info comes from social media, website, government filings, press releases, court pleadings – cases now a frequent target of attacks
Social media attacks

- Facebook – click on a link and get a pop-up saying your phone is infected, need to download an app
- Close out all programs, clear the cache, power down phone

Page at http://us.enamors377dq.pw says:

Your system is heavily damaged by Four virus!

We detect that your Samsung Galaxy S8 is 28.1% DAMAGED because of four harmful viruses from recent adult sites. Soon it will damage your phone's SIM card and will corrupt your contacts, photos, data, applications, etc.

If you do not remove the virus now, it will cause severe damage to your phone. Here's what you NEED to do (step by step):

Step 1: Tap the button and install Applock for free on Google Play!

Step 2: Open the app to speed up and fix your browser now!

WARNING!

This Samsung Galaxy S8 is infected with viruses and your browser is seriously damaged. You need
Social media attacks – May 28, 2017

- Primarily Twitter and Facebook
- Hackers spoof or imitate account of a friend
- Watch your activity online to personalize
- Got into the Pentagon
- Breached official: Wife clicked on a Twitter “family vacation” link after discussing online
- Her infection spread to his machine on home network
- 66% of such links opened
- Defense Dept. attack – 7000 clicked on an SM link
From: Dropbox [mailto:christina.seymour@hyperion-risk.com]
Sent: Friday, September 08, 2017 12:44 PM
To: John W. Simek <jsimek@senseient.com>
Subject: Invoice&wire onfirmation093.Pdf - Received

Document was sent to you via dropbox secured document sharing from your contact.

(Invoice&wireconfirmation093.Pdf)

Enjoy!

-The Dropbox
Subject: Notice to appear in Court #11272246009873

Mimecast Attachment Protection has created safe copies of your attachments.

Notice to appear in Court #11272246009873

Notice to Appear,


Do not forget to bring all the documents related to this case, attached are the Court Order and other documents pertaining this case.

PDF ID: COURTORDER090111
Caller - Number: 6344 765 3363,

You've received eFax 14 page(s) fax at 09-027-2017 05:33:31 GMT. Your electronic # for eFax document

by4_hsd58-86483871558687-5131872-91
Average user has more than 40 sites requiring password, but only 5 passwords – Experian, 2016

Security Fatigue
10 most common passwords of 2016

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 123456789
8. password
9. 123123
10. 987654321

- Power On
- Screen Saver
Password Characteristics

- Still a password driven world
- NIST new standards – Fall 2017
- Don’t need to change passwords very often – when known risk?
- Database of compromised passwords
- Use a passphrase
- 14-64 characters
- HolyswitcharooBatman!
- August 2016, NIST agreed with Carnegie Mellon – length beats complexity, special characters and upper and lower case help
Password rules

- Do not share password – 50% of employees report sharing
- Do not reuse the same password everywhere
- Troy Hunt

https://haveibeenpwned.com/
Pwned Password Database

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords exposed in data breaches. This exposure makes them unsuitable for ongoing use as they’re at much greater risk of being used to take over other accounts. They’re searchable online below as well as being downloadable for use in other online systems. Do not send any password you actively use to a third-party service - even this one!

password

pwned?

Password reuse and credential stuffing

Password reuse is normal. It’s extremely risky, but it’s so common because it’s easy and people aren’t aware of the potential impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

https://haveibeenpwned.com/Passwords
Password Managers

- LastPass – free/premium version $12 a year, multi-platform
- Keeper – Free, $29.99 per year (sync multiple devices)
- Dashlane – Free, $39.99 per year (sync multiple devices)
- PC Magazine – best password managers -2018: 
  http://www.pcmag.com/article2/0,2817,2407168,00.asp

LastPass
The Last Password You’ll Ever Need.
See or suspect something? Say something
TECHNOLOGY
Your strongest data protection

- Former FBI Director James Comey: October-December 2016, FBI took possession of 2800 devices – it couldn’t get data from 1200 of them
- First half of 2016 – 6000 devices, unable to access more than 3000
- Best protection?
- Modern encrypted devices (because their encryption has not been broken)
- Current OS
- All updates applied
Encryption – no longer cumbersome and time-consuming, now cheap, easy and maybe ethically required
Encrypt your cell phone

- Modern phones – just use a PIN
- 6 or more characters
- Samsung Galaxy S8 – fingerprint, iris scan or facial recognition (don’t use the selfie!)
Cell phone anti-malware (iPhone and Android)

- Sophos (QR Code scanner)
- Lookout
- Kaspersky
- McAfee
Beware of biometrics – the law protects something you know, not something you are
Biometrics and 2FA

- Biometrics is not a good solution – once your biometrics are owned, they will always be owned (voiceprints, fingerprints, retinas) – 5.6 million fingerprints stolen in OPM breach
- 2FA is here and growing rapidly – enable wherever you can
- Best protection? Something you know, something you have and something you are
File sharing and storage

- Dropbox – the 2012 breach still lives
- OneDrive
- iCloud
- Google Drive
- Box
- Citrix ShareFile
- SpiderOak
- Boxcryptor/Sookasa/Viivo and other bolt-ons
Confidential data needs to be shredded, NOT recycled.

Electronic data needs to be sanitized & disposed of according to best practices.
Internet of Things

- Gartner – IoT devices will exceed world’s population at end of 2018
- 7.4 billion people, 8.4 billion devices
- 20.4 billion IoT devices deployed by 2020
- All experts agree that IoT security is deplorable
- IoT is everywhere, including law firms
Drive-by infections

- Get malware by just visiting a website
- Beware of sites you don’t know
- Don’t be click-happy
Baiting – flash drives
Public computers – never use for work
Wireless

- Wi-Fi
  - Hotspots
    - WEP
    - WPA
  - WPA2
- MiFi
  - Tethering
- How do you connect safely?
  - VPN, Terminal Services — or bring up a hotspot on your phone
Secure remote access – ABA TECHREPORT
2017: 38% of lawyers use a VPN when accessing public Wi-Fi

- VPN
- Terminal Server
- Citrix
- iTwin
- Remote Control
  - LogMeIn
  - LogMeIn Ignition
  - GoToMyPC
Wireless Networks
(e.g., home networks, airports, coffee shops)

- Default values – change the defaults!
- Drive-by
- Used by spammers
- Used by neighbors to ride your access, download porn, etc.
- Hotspots
- Tunneling
Juice jacking
BYOD: Bring your own device
Apple devices are not inherently more secure than other devices.
The most common failings

- Not applying security patches or other critical updates
- Relying on outdated software for budgetary reasons – or from sheer fear of upgrading and having to learn new software!
- Using Apple devices not capable of running the latest OS
YOU play the most important part in keeping TECHSHOW exciting. *Please complete the Speaker evaluation before you leave.*

Reserve the dates!

TECHSHOW 2019: February 27 – March 2, 2019