

What Employees Need to Know About Cybersecurity



John W. Simek, Vice President, Sensei Enterprises
Michael Maschke, CEO, Sensei Enterprises

LAW OFFICE MANAGER
September 22, 2016

SHARON D. NELSON, ESQ., DAVID G. RIES, AND JOHN W. SIMEK

LOCKED DOWN

2ND EDITION

PRACTICAL INFORMATION SECURITY FOR LAWYERS

ABA LAW
PRACTICE
DIVISION

ENCRYPTION MADE SIMPLE FOR LAWYERS

DAVID G. RIES / SHARON D. NELSON / JOHN W. SIMEK

ABA LAW
PRACTICE
DIVISION

Worried about a data breach? **You should be.**



Advanced hackers with advanced tools and sufficient funds



*"You can't
defend. You can't
prevent. The only
thing you can do
is detect and
respond."*

Bruce Schneier

What we will not talk about – the IT and C-suite stuff about technology

- ❖ Firewalls
- ❖ Controlling access to data
- ❖ Security suites
- ❖ Our focus is on EMPLOYEE security awareness



Your greatest asset is also your greatest threat – your employees



The greatest misconception of employees is called “The IT Shepherd” – the belief that technology will protect them from themselves



Statistics from October 2015 study commissioned by Computing Technology Industry Association (CompTIA)

- ❖ Study of 1200 employees – 63% use work mobile devices for personal activities
- ❖ 94% use mobile business devices to connect to public Wi-Fi networks
- ❖ 78.5% use those devices to check work e-mail and 60% access work documents



Statistics from October 2015 study commissioned by Computing Technology Industry Association (CompTIA)

- ❖ 45% have never had any employee cybersecurity training
- ❖ 41% don't know what 2FA is
- ❖ 27% know the name but not how 2FA works



Statistics from October 2015 study commissioned by Computing Technology Industry Association (CompTIA)

- ❖ Salted 200 unbranded USB drives in public areas, airports, coffee shops, parks in Chicago, Cleveland, San Francisco and Washington D.C.
- ❖ 17% were picked up and used – had a trackable link and a text file to tell them to mail an e-mail address. Even IT workers did this
- ❖ This is called “baiting”



Association of Corporate Counsel: The State of Cybersecurity Report

- ❖ December of 2015, over 1000 GCs responded
- ❖ Only 1 in 3 track attendance at mandatory cybersecurity training
- ❖ Only 19% give a test
- ❖ Only 17% have “simulated security events” post-training



2015 Verizon data breach report

- ❖ 60% of cases, attackers can compromise targets in minutes
- ❖ 23% of recipients opening phishing messages and 11% clicking on attachments or links
- ❖ Attack vector:
 - 39.0% e-mail attachment
 - 37.4% e-mail link
 - 16.6% website drive-by



**“I suppose I’ll be the one
to mention the elephant in the room.”**

Holding successful training

- ❖ Morning is best – more alert
- ❖ Have coffee and food
- ❖ Make it mandatory
- ❖ Take attendance
- ❖ Engage your employees
- ❖ Sophos short YouTube videos
- ❖ Interactive
- ❖ Use contests/prizes
- ❖ Real life scenarios
- ❖ If you use a test, make those who fail repeat the test until they pass



Holding successful training

- ❖ Use a third party professional
- ❖ If you are large, your training company will probably be large
- ❖ Smaller firms use smaller (less costly) companies
- ❖ Test to measure how well people recognize danger signals in phishing e-mails
- ❖ Online training not as engaging or effective but 32% of employers use it
- ❖ Paper manuals are worthless but 15% use it
- ❖ 14.5% use one on one training (time-consuming/costly)
- ❖ 26% use in-person group workshops



How often should you train?

- ❖ At least annually – more preferred
- ❖ New technology, new threats, new defenses
- ❖ JP Morgan – Post-breach, spent a lot of money on security and training
- ❖ Tested employees a few weeks after training with phishing e-mails
- ❖ 20% failed the test
- ❖ Regularly send out alerts about new scams
- ❖ Have posters in kitchen
- ❖ Don't have a “set it and forget it” approach



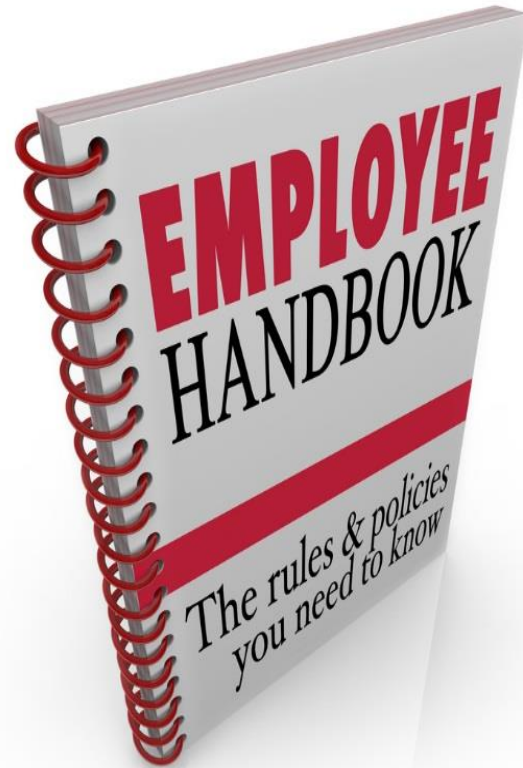
Incident Response Plan

- ❖ You have one, right?
- ❖ Let employees know the basics of the plan
- ❖ Involve some employees on periodic tabletop exercises
- ❖ Add and subtract elements of the fictional incident



Employee Policies – obey them!

- ❖ Background Checks
- ❖ Internet and E-mail Policy
- ❖ BYOD, BYON, BYOC
- ❖ Physical security
- ❖ Disaster Recovery Plan
- ❖ Encryption
- ❖ Passwords/Authentication
- ❖ Remote Access Policy
- ❖ Social Media Policy
- ❖ Incident Response Plan
 - 2015 ABA Survey
 - 28% yes
 - 47% no
 - 25% didn't know
- ❖ Monitoring and enforcement



Physical Security

- ❖ Watch for strangers in the office
- ❖ After hours, are cleaning crew really the cleaning crew?
- ❖ The infamous “Office Creeper” in the D.C. area got into many places, including a law firm



What is piggybacking?



What is tailgating?

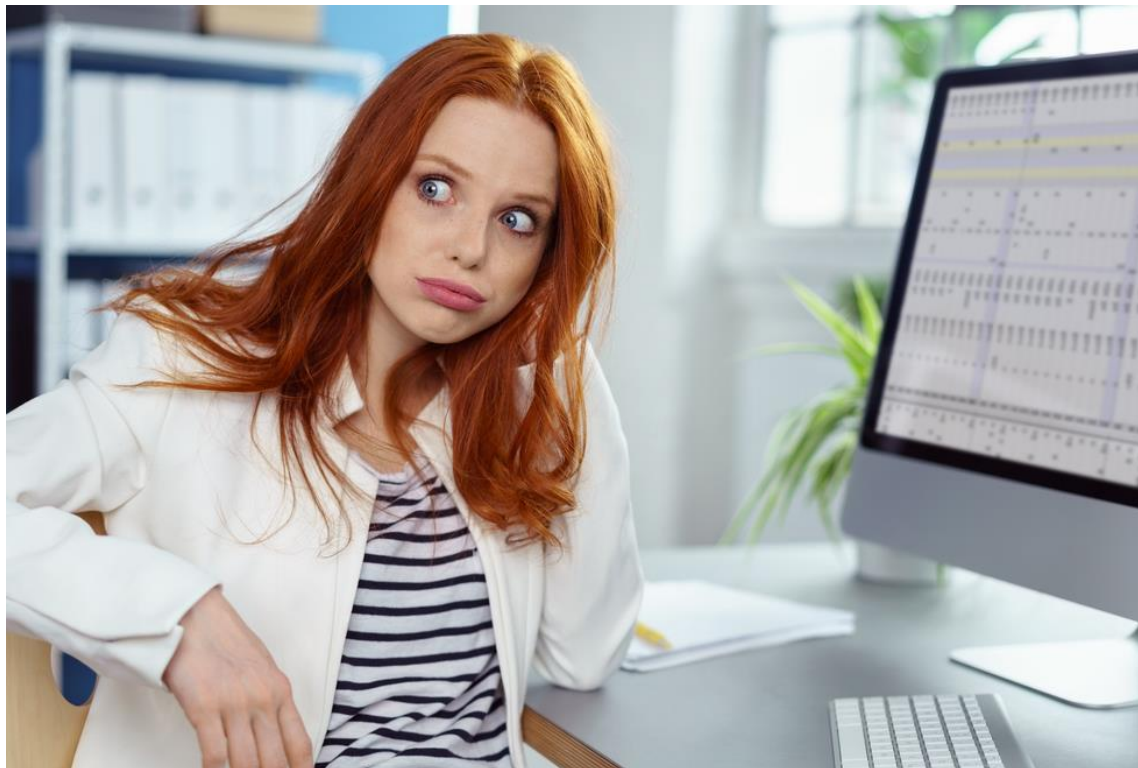


Don't be baited!



If you know another employee is engaging in insecure behavior, should you report it?

YES!!!!



Good advice to fight terrorism – and hackers



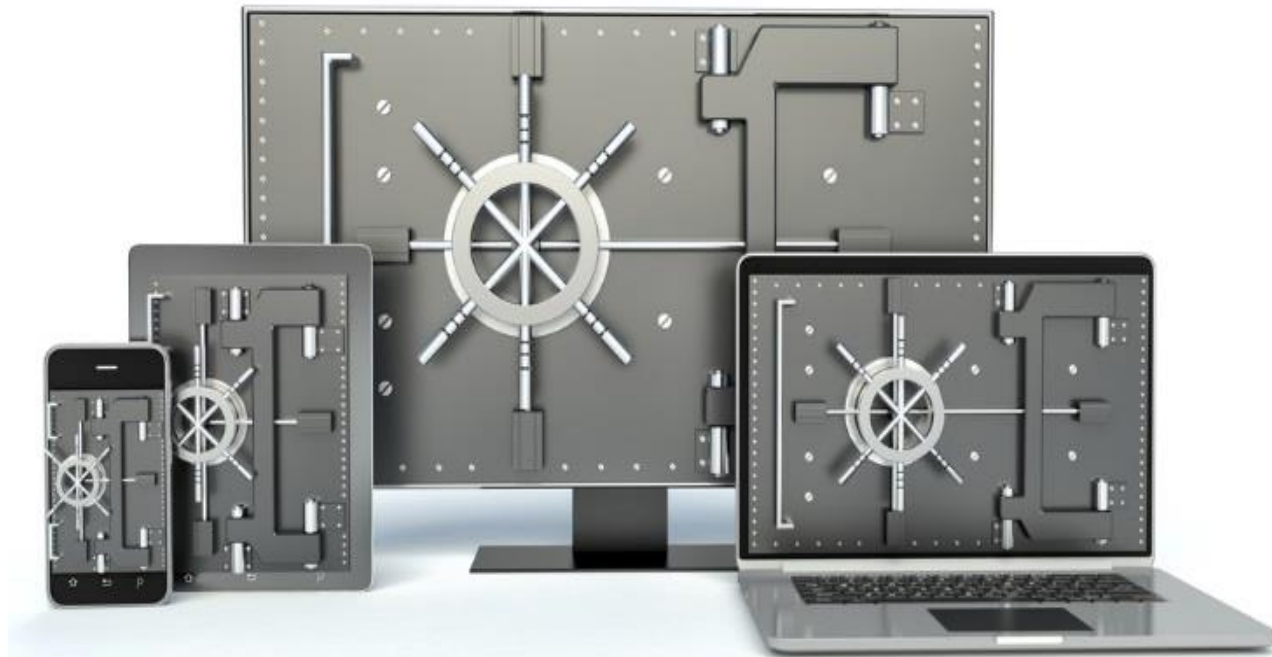
See something.
Say something.

We can't keep the barbarians at the gates

- ❖ Identify and protect – old mantra
- ❖ Now, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER



Encryption is your friend – and now it is fast,
cheap and easy



Encryption

- ❖ Encrypted in transit
- ❖ Encrypted at rest
- ❖ 2015 ABA Legal Tech Survey – only 1/3 of lawyers use encryption when sending confidential data



Encryption



- ❖ Whole Disk
- ❖ Defined Volume
- ❖ Portable Devices
- ❖ Hardware
 - Biometrics
 - TPM
- ❖ All your devices should be encrypted
- ❖ Strong PINs/passwords
- ❖ Mobile devices lost or stolen at alarming rate

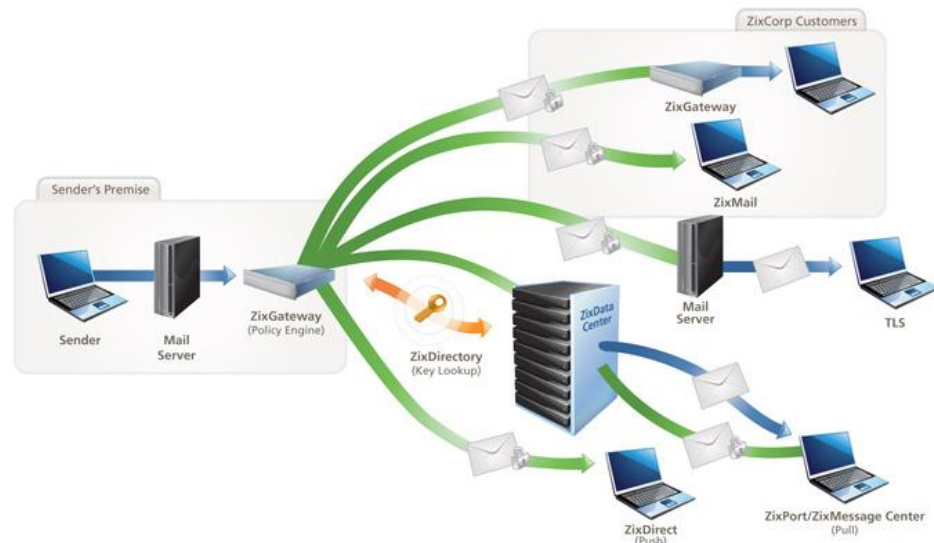
Encryption Software (if not mandated by IT)

- ❖ Symantec Encryption (PGP)
- ❖ Kaspersky Endpoint Security
- ❖ DriveCrypt Plus
- ❖ Sophos SafeGuard
- ❖ Windows BitLocker
- ❖ Mac FileVault



Encrypted e-mail – usually mandated by IT where appropriate

- ❖ ZixCorp
- ❖ Sophos
- ❖ Mimecast
- ❖ Proofpoint
- ❖ HP SecureMail
- ❖ EdgeWave
- ❖ Trend Micro
- ❖ Symantec
- ❖ Cryptzone
- ❖ DataMotion
- ❖ LuxSol
- ❖ Privato



The most common failings

- ❖ Not applying security patches or other critical updates – most of you have IT do updates for firm-wide software – do you have other software on your devices?
- ❖ Relying on outdated software for budgetary reasons – or from sheer fear of upgrading and having to learn new software!

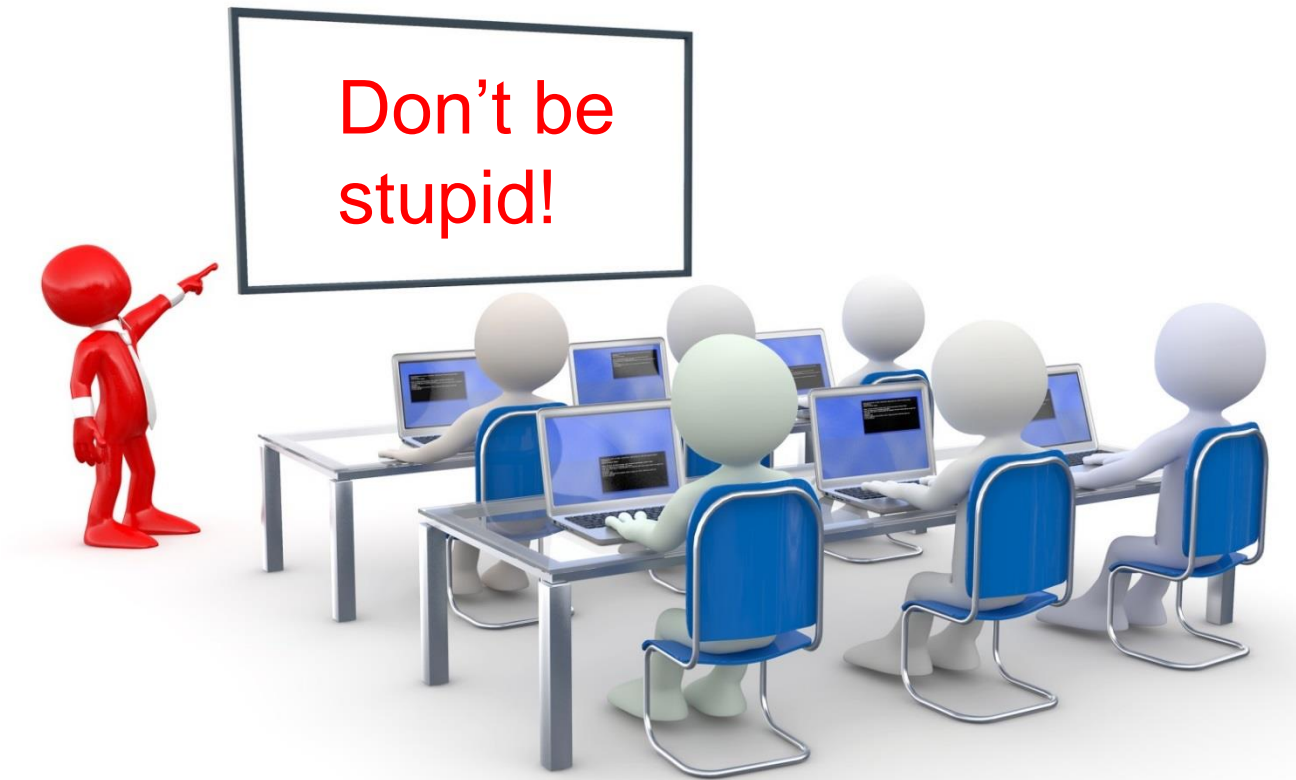


Things that make employees mad – and why they shouldn't be mad

- ❖ Application whitelisting
- ❖ Control of where you can go on the Internet
- ❖ Security policies
- ❖ Remote wiping of devices
- ❖ Not being allowed to open attachment without asking IT to release them (Freddie Mac does this)
- ❖ Policies and technology to prevent/control
 - Bring your own device
 - Bring your own network
 - Bring your own cloud



Training Training Training Have We Mentioned Training?



The user's going to pick dancing pigs over security every time.



Bruce Schneier



Social engineering

- ❖ Definition
- ❖ Highly popular technique to breach law firms
- ❖ Our desire to be helpful is not helpful to cybersecurity
- ❖ Microsoft Tech Support will never call and ask for access to your machine
- ❖ Be suspicious of a call from “your IT company” asking for your login credentials – it may not be them



Phishing

- ❖ Definition
- ❖ Enterprise anti-malware software doesn't catch everything – there are zero day exploits sold on the Dark Web
- ❖ Employees will open 20% of phishing e-mails according to one study
- ❖ German study showed curiosity a big factor
- ❖ E-mail promising photos of wild New Year's Eve party – 34% opened out of curiosity even though they didn't know the sender!



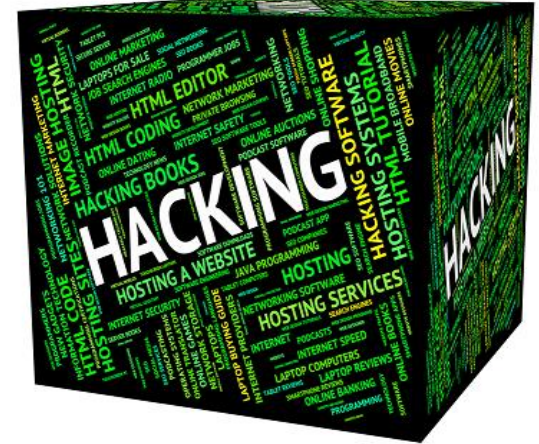
Targeted phishing

- ❖ Definition
- ❖ Law firms at a disadvantage – much legal data is public
- ❖ Law firms also a “honey pot” because they hold the data of so many clients
- ❖ Hackers may know managing partner’s nickname or know (and spoof) e-mail addresses of clients, other attorneys and courts
- ❖ Suspicious e-mail? Check with IT



Business e-mail compromise a/k/a CEO scam


- ❖ Directed to someone who can wire money
- ❖ Appears to come from someone who has authority to order wire transfers
- ❖ ALWAYS question any instruction to wire significant funds
- ❖ If you blow it, those funds may be lost forever
- ❖ And if they are from a trust account, arrrrgh, the ethical and legal implications are profound
- ❖ FBI reports over 3 billion dollars lost to date
- ❖ From Jan. 2015 – June 2016, increase of 1500% in successful attacks





How to spot a phishing e-mail

- ❖ From someone you don't know
- ❖ Nothing in the note seems personal to you
- ❖ You weren't expecting the e-mail
- ❖ Reference made to a bank/product/service you don't use
- ❖ Poor English/misspellings
- ❖ Even if you know the sender, look for one letter misspelled in the sender's e-mail
- ❖ Hovering over a link in an e-mail doesn't necessarily tell you where it goes – drive-by malware may be waiting
- ❖ Never enable macros if requested to do so



Allways chek for
spelning errors

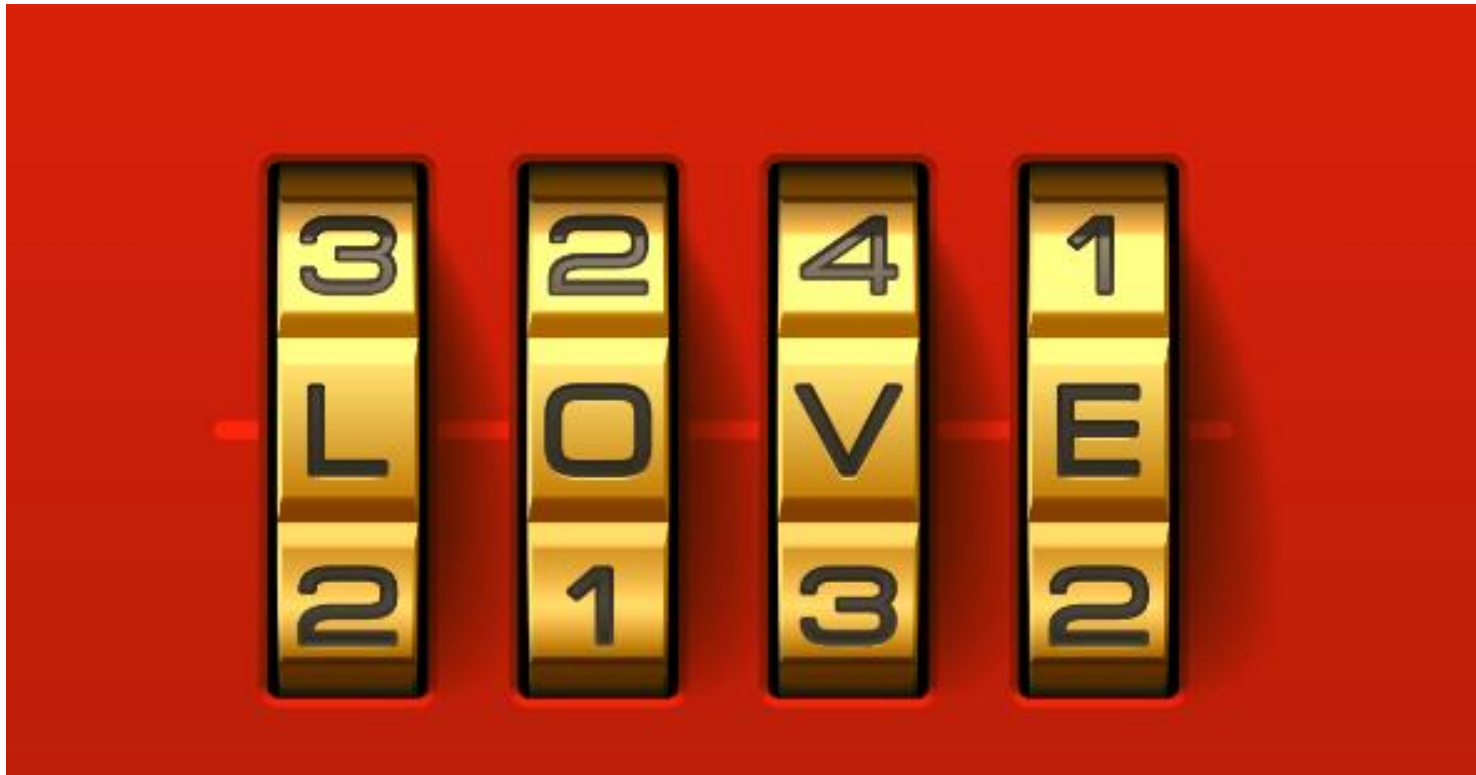
How do you know if you have malware?

- ❖ You often don't
- ❖ Some signs to report:
 - Sudden slowness
 - Strange message appearing on screen
 - Inability to open a file
 - Pop-ups on screen
 - Machine crashing
 - Running out of hard drive space
 - High volume of machine activity
 - New browser, new home page, new tool bar you didn't install
 - New programs that start automatically



Passwords

- ❖ Don't share them (configure authorization instead)
- ❖ Don't reuse them (hacked once, hacked everywhere)
- ❖ No easily guessed/cracked passwords



The Ashley Madison breach – password lessons

Members Login ▾

ASHLEY MADISON®


Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select ▾

See Your Matches »


Over **41,330,000** anonymous members!




★★★★★
100%
Like-minded
People

As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for **discreet** encounters

 Trusted Security Award

100% DISCREET SERVICE

 SSL Secure Site

[Register on Ashley Madison](#) [Affiliate Program](#) [Press](#) [FAQ](#) [Guarantee](#) [Blog](#) [Infidelity News](#) [Articles](#) [Terms](#) [Privacy](#) [Contact Us](#)

Follow Ashley Madison on: [Twitter](#) [Facebook](#) [Youtube](#)

Location: [USA](#) ▾ Language: [English](#) ▾

Ashley Madison is the most famous name in infidelity and married dating. As seen on Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today. Ashley Madison is the most recognized and reputable **married dating company**. Our Married Dating Services for Married individuals Work. Ashley Madison is the most successful website for **finding an affair** and cheating partners. Have an Affair today on Ashley Madison. Thousands of **cheating wives** and cheating husbands signup everyday looking for an affair. We are the most famous website for **discreet encounters** between married individuals. Married Dating has never been easier. With Our affair guarantee package we guarantee you will find the perfect affair partner. Sign up for Free today.

© 2001 - 2015 Avid Dating Life Inc.

18+ Adult Dating means that all members must be 18 years or older

[Sitemap](#)



Who
Wants
To
Hack
Me

- ❖ 123456
- ❖ 12345
- ❖ Password
- ❖ DEFAULT
- ❖ 123456789.

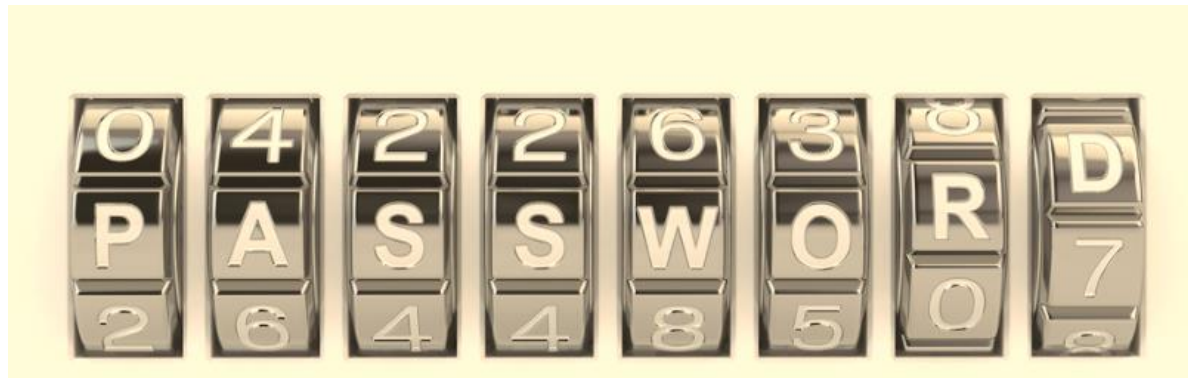
Password Characteristics

- ❖ Still a password driven world
- ❖ Alphanumeric
- ❖ Special characters
- ❖ Use a passphrase
- ❖ Length – 14 characters
- ❖ Ihavebeen-andalwaysshallbe-yourfriend.22715



New rules from NIST (still in draft form)

- ❖ Length is more important than complexity
- ❖ Recommends passphrases
- ❖ 16-64 characters in length
- ❖ Longer passphrases for log-in, screen saver and financial passwords
- ❖ Don't write passwords on sticky notes
- ❖ Don't keep a "Passwords" file on your device unless it is encrypted



No e-mail encryption? How do you encrypt a document you attach to an e-mail?

- ❖ You password protect it – the OPEN password
- ❖ Word, PDF, Zip file – Encrypt with password

The screenshot shows the Microsoft Word 2010 interface. The 'File' tab is selected on the ribbon, displaying the 'Save', 'Save As', 'Open', 'Close', 'Info', 'Recent', 'New', 'Print', 'Save & Send', and 'Help' options. The 'Info' option is currently selected, opening the 'Information about Document1' pane. This pane is divided into three sections: 'Permissions', 'Prepare for Sharing', and 'Versions'. The 'Permissions' section shows a 'Protect Document' button and states that 'Anyone can open, copy, and change any part of this document.' The 'Prepare for Sharing' section shows a 'Check for Issues' button and lists 'Author's name' as a potential issue. The 'Versions' section shows a 'Manage Versions' button and states 'There are no previous versions of this file.' On the right side of the ribbon, the 'Document1 - Microsoft Word' title bar is visible, along with a preview of the document and a 'Properties' pane showing details like 'Size', 'Pages', 'Words', 'Total Editing Time', 'Title', 'Tags', 'Comments', 'Related Dates', and 'Related People'.

Document1 - Microsoft Word

File Home Insert Page Layout References Mailings Review View

Save
Save As
Open
Close
I Info
Recent
New
Print
Save & Send
Help
Options
Exit

Information about Document1

Permissions
Anyone can open, copy, and change any part of this document.

Protect Document ▾

Prepare for Sharing
Before sharing this file, be aware that it contains:

- Author's name

Check for Issues ▾

Versions
There are no previous versions of this file.

Manage Versions ▾

Properties ▾

Size	Not saved yet
Pages	1
Words	1
Total Editing Time	0 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	Never
Created	Today, 10:25 AM
Last Printed	Never

Related People

Author	Sharon D. Nelson Add an author
Last Modified By	Not saved yet

[Show All Properties](#)

Do not send passwords in an e-mail!



Password Managers

- ❖ LastPass – free/premium version \$12 a year, multi-platform
- ❖ eWallet - \$19.99, \$9.99 for mobile platforms
- ❖ Keeper - \$29.99 per year
- ❖ PC Magazine – best password managers -2016:
<http://www.pcmag.com/article2/0,2817,2407168,00.asp>

LastPass 
The Last Password You'll Ever Need.

Biometrics and 2FA – what is 2FA and how does it work?

- ❖ 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, so that you are using a password and 2FA
- ❖ Best protection? Something you know, something you have and something you are



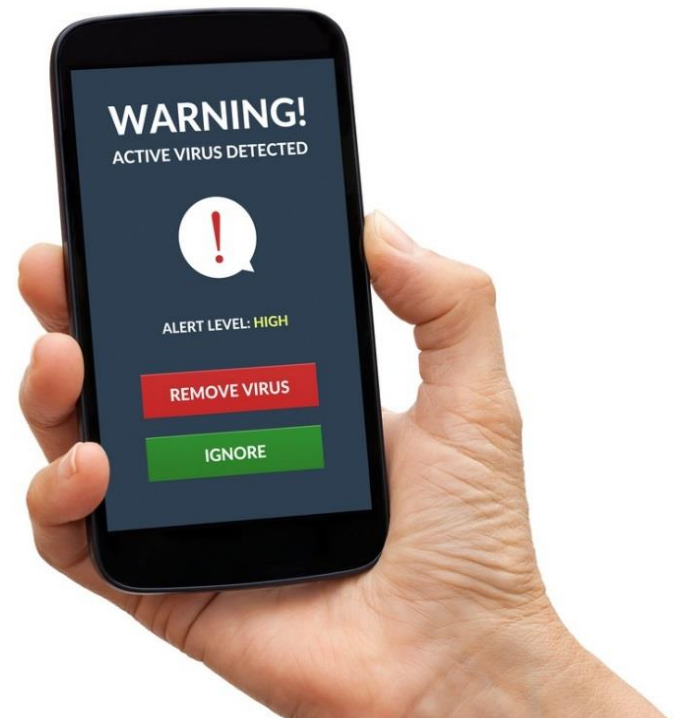
Ransomware



- ❖ How do you get it?
- ❖ What does it do?
- ❖ How do you get your data back?
- ❖ How do you engineer backups that are impervious to ransomware?
- ❖ 4000% increase in 2014
- ❖ 165% increase in 2015

Ransomware attacking mobile devices

- ❖ Began in 2015 and growing
- ❖ Downloading apps from unsanctioned app stores
- ❖ Simple fix – don't do it!!!!



Remember to scrub metadata

- ❖ It should be on by default
- ❖ Disable only when tracked changes need to be shown in collaborating



Cloud Services – who holds the decryption key? Governed by policy or tech?

- ❖ Dropbox
- ❖ OneDrive
- ❖ iCloud
- ❖ Google Drive
- ❖ Box
- ❖ SpiderOak
- ❖ Bolt on products – Viivo, Boxcryptor, Sookasa



Social media

- ❖ Suggested posts
 - Prince's last moments captured in video!
 - We know why Oprah is crying in this photo!
 - They found the Malaysian airliner!
 - Don't let curiosity kill you!



Apple devices are no more secure than other devices. They never were. They still aren't. That is all.



Public computers – never use for work

Hotel business centers, public libraries, Internet cafes



Secure remote access

- ❖ VPN
- ❖ Terminal Server
- ❖ Citrix
- ❖ iTwin
- ❖ Remote Control
 - LogMeIn
 - LogMeIn Ignition
 - GoToMyPC



Wireless Networks

- ❖ Default values – change the defaults!
- ❖ Drive-by
- ❖ Used by spammers
- ❖ Used by neighbors to ride your access, download porn, etc.



Wireless



- ❖ WiFi
 - ~~WEP~~
 - ~~WPA~~
 - WPA2
- ❖ MiFi
 - Tethering
- ❖ How do you connect safely?
VPN – or bring up a hotspot on your phone

Smartphones



- ❖ Encryption – how to
- ❖ PIN – 6+ characters
- ❖ Password is better
- ❖ Even if you don't save things to the phone, it may auto-save
- ❖ Security Policy
- ❖ Remote Wipe
- ❖ Memory Cards
- ❖ Texting
- ❖ PIN-to-PIN
- ❖ iMessage

Cell phone anti-malware (iPhone and Android – your IT folks may mandate what you use)

- ❖ Sophos
- ❖ Lookout
- ❖ Kaspersky
- ❖ McAfee
- ❖ Can't protect iPhone's kernel



Vendor management: What are we outsourcing?

Duty to supervise and ensure security!

- ❖ Payroll
- ❖ Virtual paralegals
- ❖ Virtual receptionists
- ❖ Backup
- ❖ Case management



DANCE LIKE NO ONE'S WATCHING.
ENCRYPT LIKE EVERYONE IS!



Questions?

