

CYBERSECURITY... MORE THAN A PASSWORD

Michelle Swift, RN, JD, CPHRM
Patient Safety Risk Manager

June 3, 2017

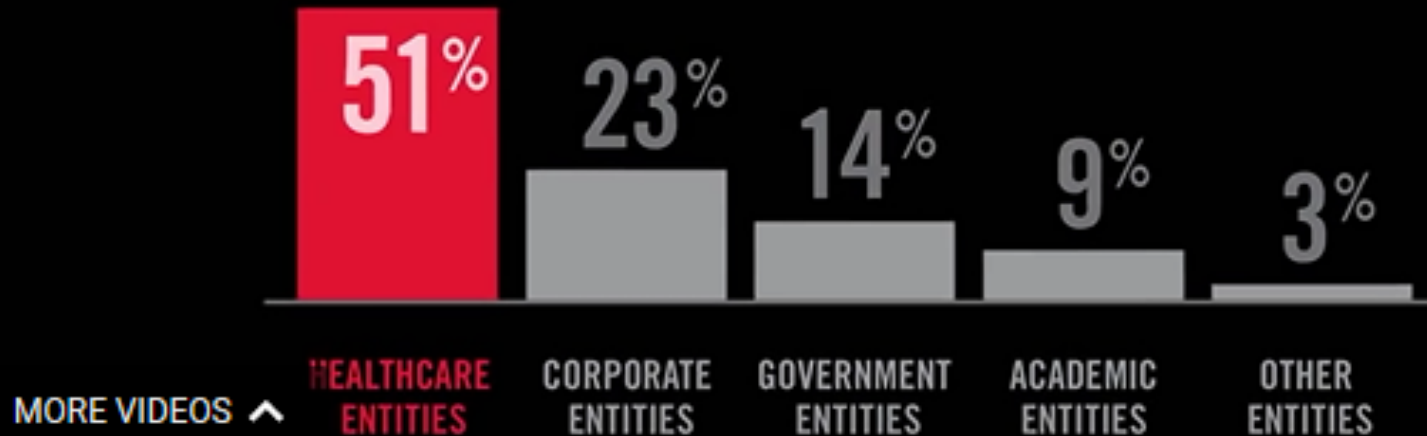
OBJECTIVES

- Identify internal and external threats to data security that exist in our healthcare environment
- Define data breach and the steps required of breach notification laws
- Create a step-by-step plan to assess your risk of a data breach

HEALTHCARE IS MOST VULNERABLE

Case Studies: Healthcare Data Breach Risks

PERCENTAGE OF TOTAL BREACHES THAT OCCUR IN:



EXPOSURE TO DATA BREACHES

2017 DATA BREACHES

In 2016, Yahoo announced the largest data breach in history affecting more than one billion accounts...

- Major hacks in 2017...
 - Chipotle
 - InterContinental Hotels Group
 - FAFSA: IRS Data Retrieval Tool for student aid application
 - University North Carolina Health Care

WYOMING HOSPITAL

Potential Healthcare Data Breach Due to Phishing Scam

- Approximately 3,184 individuals were notified that their protected health information may have been accessed by an unauthorized user
- An outside entity gained access to two email accounts in the organization
- The entity first sent a phishing email to only one employee—after the employee opened the email, the entity was able to use the employee's account to send more phishing emails to other staff
- One other email account was compromised, which caused the entity to have access to the organization's email for 15 minutes
- Wyoming Hospital notified affected individuals of the possible healthcare data breach, reinforced employee training, and revised policies

WHY?

Hacker service	Price
Social Security number (sold as part of 'Fullz' dossier)	\$30
Date of birth	\$11
Health insurance credentials	\$20
Visa or MasterCard credentials	\$4
American Express credentials	\$7
Discover credit credentials	\$8
Credit card with magnetic stripe or chip data	\$12
Bank account number (balance of \$70,000 to \$150,000)	\$300 or less
Full identity 'Kitz'	\$1,200 to \$1,300

SHOULD YOU WORRY ABOUT A DATA BREACH?



Yes.

**It is not a question of if,
but when...**



**A data breach can
significantly impact
your reputation and
potentially your financials.**

HOW IS THE BREACH LIKELY TO HAPPEN?

- **Social Engineering:** psychological manipulation to perform actions or divulge confidential information
 - Traditional or personal approach
 - Banking—important security issue
 - Phone call—“I’m from Microsoft...”
 - Urgent—“Just click on this link...”
 - Trending: industry specific
- **Physical Access:** information at office or home
 - User identification and password on sticky note or in desk drawer
 - Sensitive documents placed in the dumpster



Social Engineering Example #1

Exclusively for: | VALUED CUSTOMER
Online Banking



Your Bank of America accounts has been locked!

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Please [click here](#) to continue the verification process and ensure your account security.



Email Preferences

This is a service email from Bank of America. Please note that you may receive service email in accordance with your

- Call to action
- Spear phishing email from Bank of America
- Action
 - Delete email
 - Call Bank of America or log in to Bank of America online account

Social Engineering Example #2

Tax Refund

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: IRS
To: IRS
Subject: Tax Refund

Internal Revenue Service
United States Department of the Treasury

Tax Refund
Get your Tax Refund on your VISA or MasterCard

Please enter your Social Security Number and a valid Credit / Debit Card where you want the refund to be made.
*See our [Privacy Notice](#) regarding our request for your personal information.

Social Security Number
or IRS Individual Taxpayer Identification Number [shown on your tax return](#)

Credit / Debit Card
Please enter the following information here:

Personal Information
Please enter the following information here.

Form Fields:

- SSN: [] - [] - []
- Name on Card: []
- Card Number: []
- Expiration Date: [mm] / [yy]
- Cvv Code: []
- Date of Birth: [mm] / [dd] / [yy]
- Address: []
- City: []
- Zip Code: []
- Phone Number: []
- E-mail Address: []

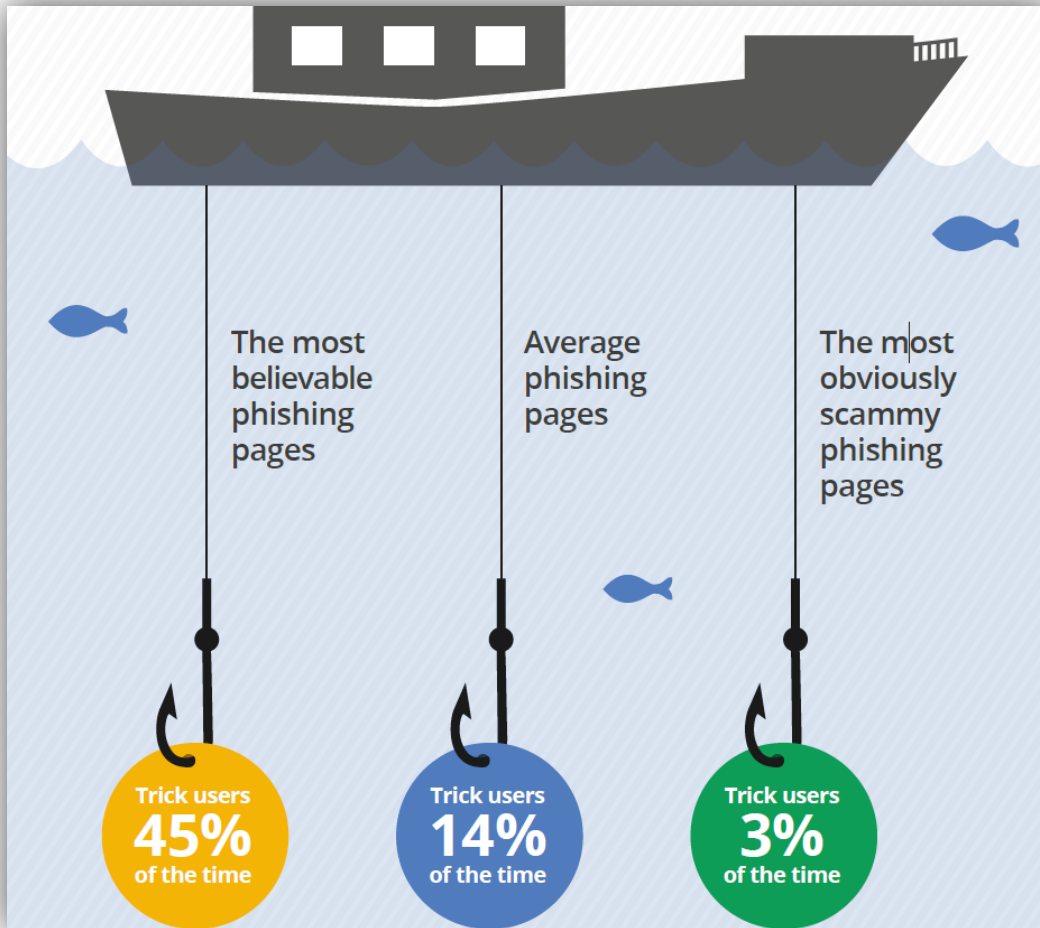
Submit

Note: For security reasons, we recommend that you close your browser after you have finished the refund process.

[IRS Privacy Policy](#)

- Information request
- Phishing email from Internal Revenue Service (IRS)
- Action
 - Delete email
 - Call IRS or log in to IRS online account

SOCIAL ENGINEERING: MALWARE IS A MAJOR PROBLEM



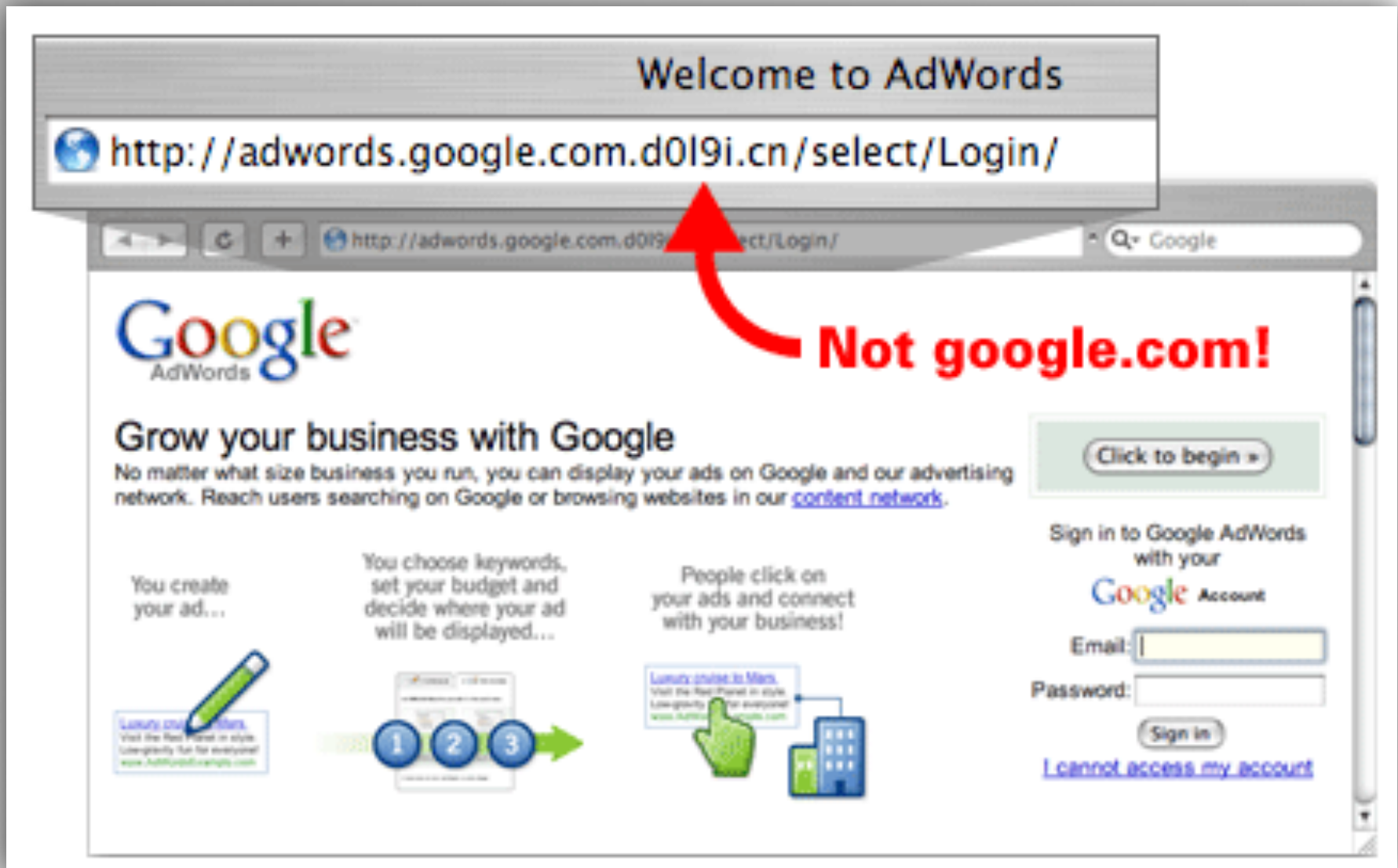
- Most common attack vector is spear phishing emails
- Attempt to gain access to a computer network by having a user click on a hyperlink or execute a program
- Malware used to mine bitcoins

STEPS TO AVOID SPEAR PHISHING RISKS

Ask...

- Have I ever received something like this from the sender?
- Does the email appear grammatically correct?
- Does the email address me by name?
- Is there a sense of urgency or critical call to action within a specific time frame?
- Are there hyperlinks or attachments to open?
- Is the URL authentic? **http://host.name/path**
- Is there another way to access the information?

Note the URL Address



The screenshot shows a web browser window with the address bar displaying `http://adwords.google.com.d0l9i.cn/select/Login/`. A red arrow points from the text "Not google.com!" to the address bar. The page content includes the Google AdWords logo, the heading "Grow your business with Google", and a sign-in section with fields for email and password. A diagram on the left illustrates the AdWords process: "You create your ad..." (1), "You choose keywords, set your budget and decide where your ad will be displayed..." (2), and "People click on your ads and connect with your business!" (3).

Welcome to AdWords

`http://adwords.google.com.d0l9i.cn/select/Login/`

Google AdWords

Grow your business with Google

No matter what size business you run, you can display your ads on Google and our advertising network. Reach users searching on Google or browsing websites in our [content network](#).

Click to begin »

Sign in to Google AdWords with your Google Account

Email:

Password:

Sign in

[I cannot access my account](#)

You create your ad...

You choose keywords, set your budget and decide where your ad will be displayed...

People click on your ads and connect with your business!

1 2 3

ALBUQUERQUE LOSES \$420,000 IN ELECTRONIC WIRE FRAUD

The city discovered that it had fallen victim to a scam...

Office of the State Auditor said in a news release that the city had complied with a fraudulent request to change vendor payment information that diverted the public funds to the scammer via the Internet.



PHYSICAL ACCESS

Building Access SEAL: Shred, Encrypt, No Access, Lock

- Secure access
- Lock all cabinets and digital devices
- Encrypt all computers/portable devices
- Remove passwords from sticky notes
- Shred paper documents
- Secure external dumpster



(continued)

PHYSICAL ACCESS

Skimming

- Pocket sized scanner skims credit card information
- May attach a phony card reading device to ATM, gas pump, etc.
- May send or deliver a “new” credit card device to replace your current device



CASE STUDY #1

The office staff frequently uses sticky notes to write messages and track patients information.

These notes often have protected health information written on them. At the end of the day the office does not have a system to ensure the note is shredded. A local person goes through the dumpster and identifies patients' information and reports this to the Office of Civil Rights.



CASE STUDY #2

UPS delivers a new credit card machine with instructions on how to replace your current machine. No one in your office remembers hearing anything about the credit card company sending a replacement and the new machine looks similar to the current machine.

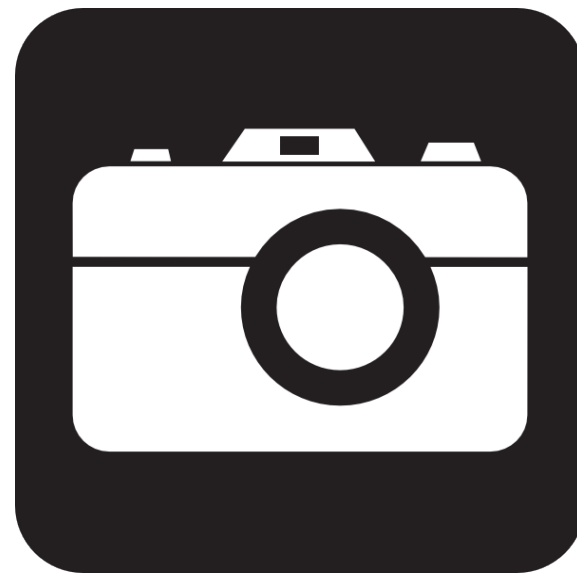
What is the potential problem here?

CASE STUDY #3

Plastic surgeon takes before and after photos of his patients. One afternoon during office hours the fire alarm rings requiring evacuation of everyone in the multi-office building.

Upon returning to the office the surgeon realizes the camera is not on the counter where he is certain he left it prior to evacuating the building.

What now?



MOBILE DEVICE RISKS

- Balance risks and convenience
- Establish policies
- Restrict applications—e.g., accessing internal applications from personal devices
- Use security features, tracking applications, auto locking, etc.
- Beware of eavesdropping
- Be aware of theft
- Dispose of properly—sanitize

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

Southern California hospital became another victim of ransomware—an attack where the computer system is held hostage by cybercriminals until a ransom is paid. Demanded \$17,000 ransom to restore its systems and functions.

What are your options in this situation?

THREE OPTIONS IN A RANSOMWARE ATTACK

- Restore from the recent system backup
 - Pay ransom if backup is not available
 - Put system back to default setting—lose everything
-
- ***Note: Encryption does not protect you from a ransomware attack.***

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

(continued)

“The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key,” said the CEO of the medical center. “In the best interest of restoring normal operations, we did this.”

PREVENTING RANSOMWARE ATTACK

- Security training for all employees
- Move systems—both software and data to the cloud
- Data should be encrypted when stored in cloud
- Understand access to your cloud data
- Understand options if cloud is hacked or data is lost—look at service agreement
- Block malware
- Install intrusion detection software to monitor illegal activities on networks
- Perform regular system back ups—hourly for critical systems

DATA BREACH NOTIFICATION

SAFE HARBOR

Encryption = No Breach



DEFINITION OF “BREACH” IN HIPAA FINAL RULE

- Acquisition, access, use, or disclosure of unsecured protected health information (e.g., social security, credit card, date of birth) in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach...unless the Covered Entity or Business Associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment...
- *Compromise* is not defined

STEPS OF BREACH NOTIFICATION

According to HIPAA...

- Who must be notified
 - Patient or their personal representative, HHS, and the media (if more than 500 residents of a state or jurisdiction are affected)
- Notification timeframe
 - Without unreasonable delay and in no case later than sixty (60) calendar days after the breach is discovered
- Notification is very specific
- Preemption
 - HIPAA preempts state law unless state law is more restrictive

WRITTEN NOTIFICATION OF BREACH

According to HIPAA...

- Covered entities must provide individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically within 60 days of discovery
- If the covered entity has insufficient or out-of-date contact information for 10 or more individuals there are alternative options

CASE STUDY #1

Physician takes home 12 paper medical records to work on over the weekend. He leaves them in his pickup truck which is unlocked and parked near his home. He always leaves the keys in the ignition.

Saturday night while at dinner he receives a call from the local police. Several teenage boys had taken his truck for a joyride and the truck was found near the city park.

What should the physician do now?

CASE STUDY #2

Patient is scheduled for an elective procedure at the nearby surgical center. Per office protocol the patient's history and physical, consent, and pre-operative medical records are sent over to the surgical center.

Patient calls the office and complains about a "HIPAA breach" and demands something be done about the breach.

What should the physician do?

CASE STUDY #3

Billing company notifies the physician through their attorney that 60 of the physician's patients had their information breached when the billing company's file server was compromised 58 days ago. The investigation into the breach indicated that treatment reports with names, addresses, and social security numbers were compromised.

What are the issues here?

CASE STUDY #4

Pediatrician scans the medical record in his office for names and addresses for neighborhood children to invite to his daughter's birthday party.

What are the issues here?

WYOMING STATE PRIVACY LAWS

WYOMING STATE LAW

- Right of access for copy of medical record within 30 days (hospitals within 10 days)
- Fees allowed including postage
- Right to amend medical record
- Right to file a complaint with Office of Civil Rights
- Sue in state court for violation of rights under state law
 - No federal cause of action
- Right to file a Wyoming Board of Medicine complaint





PRACTICE TIPS

PRACTICE TIP: ENFORCEABLE POLICIES AND PROCEDURES

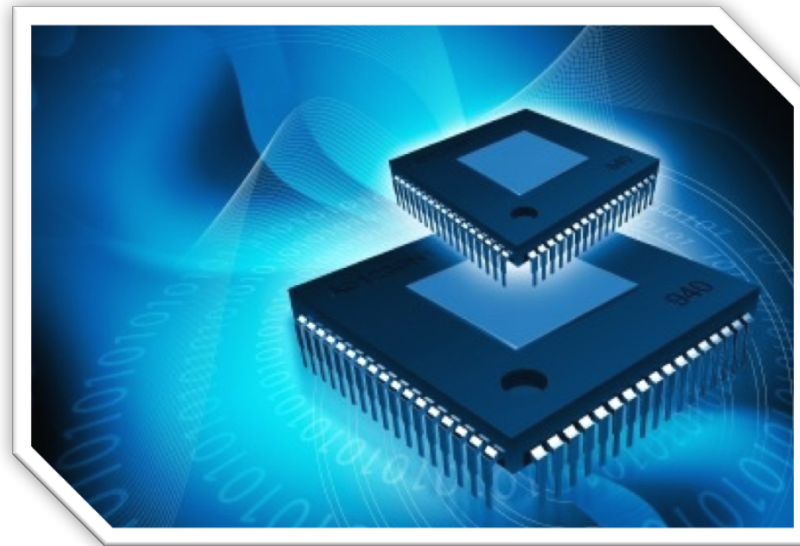


PRACTICE TIP: STAFF TRAINING



PRACTICE TIP: ENCRYPTION

- Encryption (free: Windows 8 Pro)
 - Desktop and servers
 - Verify USB devices
 - Tablets
 - Laptops
 - Cell phone



PRACTICE TIP: PASSWORDS

- Never use the same username/password combination at work and at home
- Increase complexity of password (e.g., ISnowskeee2@Jacks0n)
- Google “how secure is my password”



PRACTICE TIP: DATA RECOVERY PLAN



PRACTICE TIP: PHYSICAL AND ELECTRONIC ACCESS

- Physical access to office and protected health information
 - Secure access to office
 - Lock cabinets
 - Shred key paper documents
 - Lock up digital devices (e.g., camera)
 - Secure external dumpster
- Vendors
 - Actively manage all vendor access credentials



PRACTICE TIP: SEPARATE WIFI FOR GUESTS



PRACTICE TIP: UPDATE SOFTWARE

- Antivirus protection
- Anti-malware
- Spyware
- Trojans
- Firewall
- Adware



PRACTICE TIP: CYBER INSURANCE



RESOURCES

- U.S. Department of Health & Human Services Office for Civil Rights
 - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
 - www.hhs.gov
- Security Risk Assessment Tool
 - www.healthit.gov

Michelle Swift, BSN, JD, RN, CPHRM

Patient Safety Risk Manager

Department of Patient Safety and Risk Management

Northwest Region

mswift@thedoctors.com

(800) 421-2368, ext. 6355

THANK YOU

We relentlessly defend, protect, and reward
the practice of good medicine.

