Sharp HealthCare's 2014 Compliance Education Module 4

Stay Connected. Stay Secure.

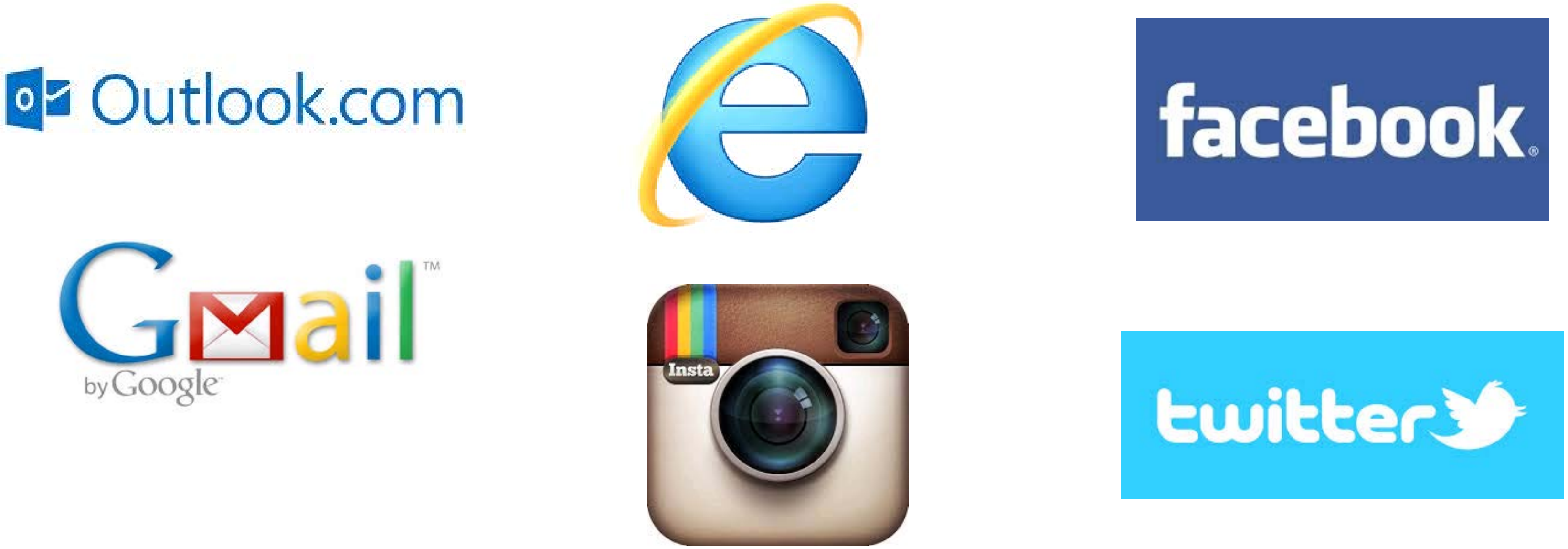
Balancing productivity and security in a connected world

Your Daily Routine

More than likely, checking your email and using the Internet is crucial to your daily work routine.

Connected for Communication

Think of all of the ways you communicate in your personal life …



Connected at Work

Staying connected is also critical to the workplace, especially at Sharp.

Stay Connected. Stay Secure.

- Of course, this connectivity comes with a level of risk.
- The convenience that connectivity provides needs to be balanced with an appropriate level of security.
- If not, it could potentially expose sensitive patient or employee data, resulting in a reportable breach.

- What are some of these risks? And more importantly, how can you reduce the risk of a compromise?

Phishing

- What is phishing?
  - Phishing (pronounced “fishing”) is a type of scam designed to steal your information.
  - It commonly involves email and phony websites that appear legitimate, but inappropriately ask you to share sensitive information such as credit card numbers, passwords, account data, or other information.
- Consider a recent example of how responding to a phishing scam resulted in serious breach of patient data.

Phishing in the News

- California's UC Davis Health System recently began notifying approximately 1,800 patients that their personal or medical information may have been exposed when three UC Davis physicians' e-mail accounts were *compromised by phishing attacks* in mid-December of 2013.
- Information in the e-mails included names, medical record numbers and limited information associated with a clinic visit or hospital admission.

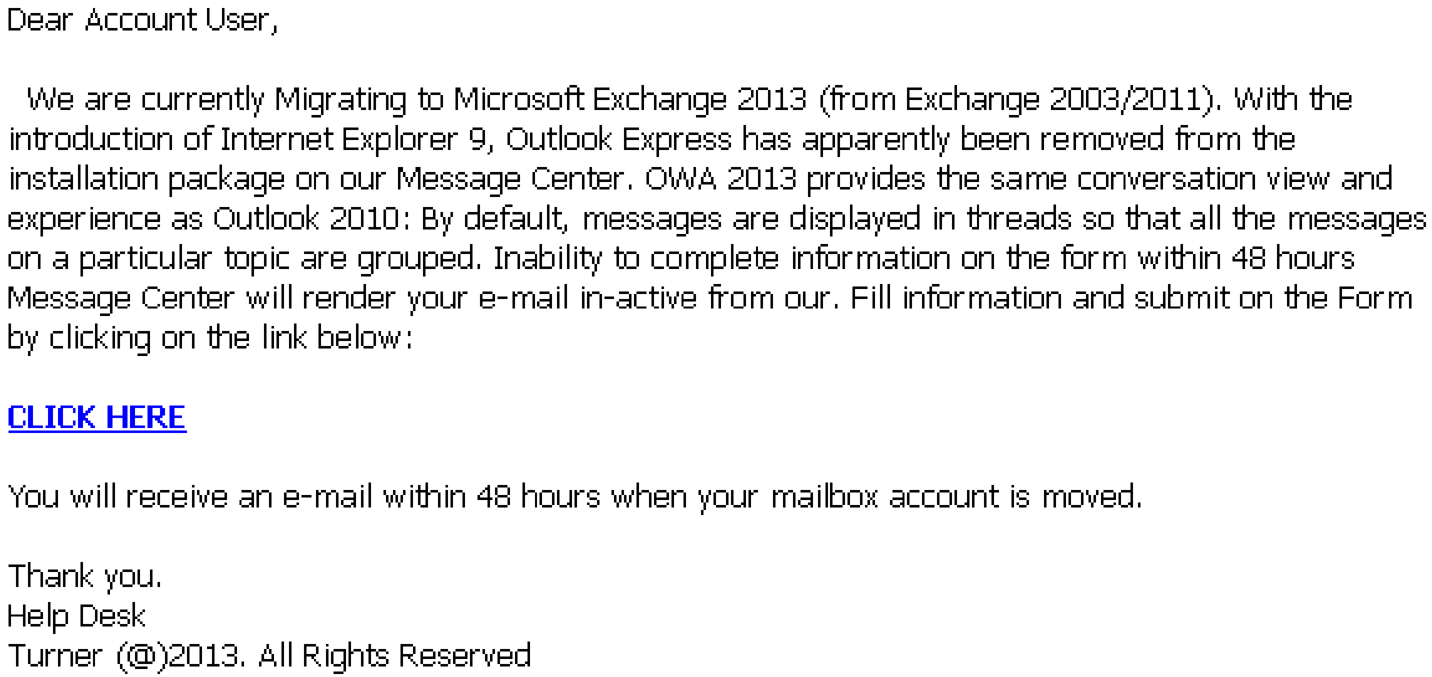
Source: http://www.esecurityplanet.com/network-security/phishing-attacks-expose-1800-uc-davis-patients-data.html

Protect Yourself From Phishing

- The risks associated with phishing are very real.
- How can you avoid becoming a victim of phishing?
- One way is to learn how to recognize and respond to a phishing attempt.

How to recognize a phishing email

Look carefully. How many signs of phishing can you find in this example?



Dear Account User,

We are currently Migrating to Microsoft Exchange 2013 (from Exchange 2003/2011). With the introduction of Internet Explorer 9, Outlook Express has apparently been removed from the installation package on our Message Center. OWA 2013 provides the same conversation view and experience as Outlook 2010: By default, messages are displayed in threads so that all the messages on a particular topic are grouped. Inability to complete information on the form within 48 hours Message Center will render your e-mail in-active from our. Fill information and submit on the Form by clicking on the link below:

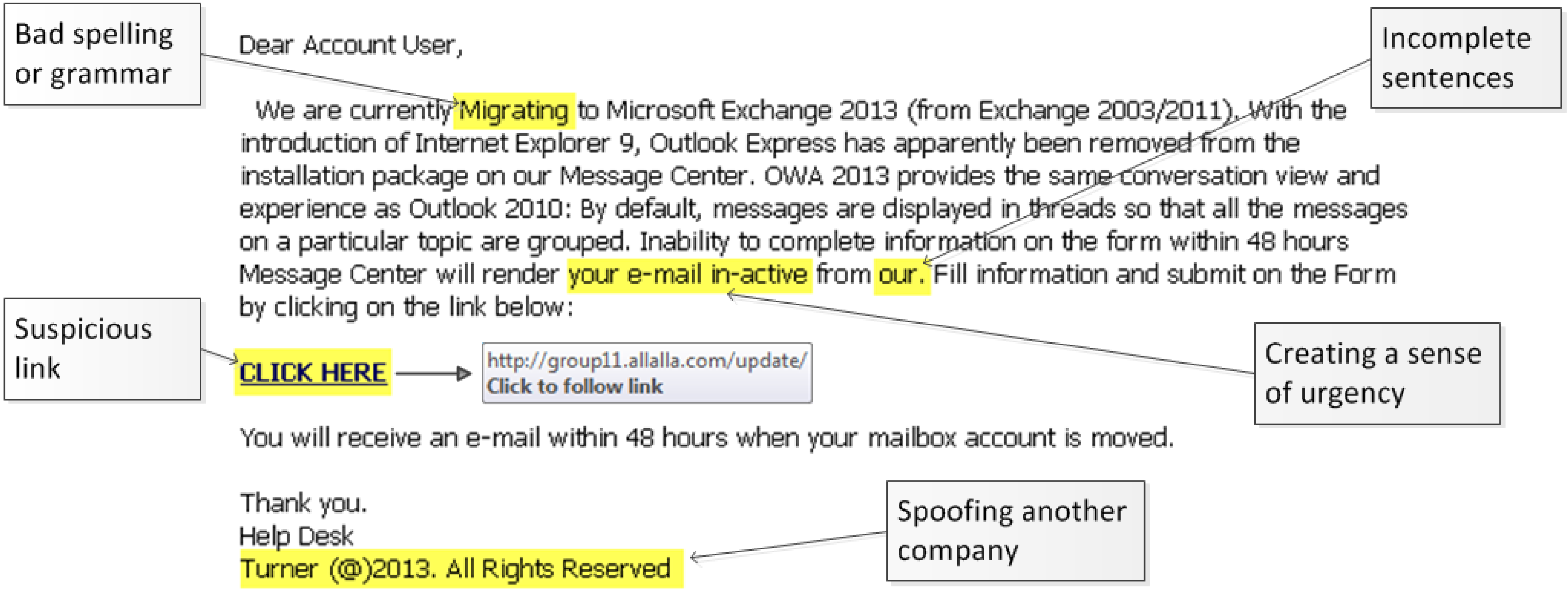
CLICK HERE

You will receive an e-mail within 48 hours when your mailbox account is moved.

Thank you.
Help Desk
Turner (@)2013. All Rights Reserved

Signs of a phishing email

Here are a few signs to help you recognize a phishing email.



Bad spelling or grammar

Incomplete sentences

Dear Account User,

We are currently Migrating to Microsoft Exchange 2013 (from Exchange 2003/2011). With the introduction of Internet Explorer 9, Outlook Express has apparently been removed from the installation package on our Message Center. OWA 2013 provides the same conversation view and experience as Outlook 2010: By default, messages are displayed in threads so that all the messages on a particular topic are grouped. Inability to complete information on the form within 48 hours Message Center will render your e-mail in-active from our. Fill information and submit on the Form by clicking on the link below:

Suspicious link

CLICK HERE → http://group11.allalla.com/update/
Click to follow link

Creating a sense of urgency

You will receive an e-mail within 48 hours when your mailbox account is moved.

Thank you.
Help Desk
Turner (@)2013. All Rights Reserved

Spoofing another company

How to respond to a suspicious email

- If you receive a suspicious looking email:
  - Delete it, especially is if contains signs of phishing.
  - Do not reply or click on any links in the email.
  - Do not open any attachments, as they may contain viruses or other harmful software.
  - Do call (858) 627-5000 or email the Technical Assistance Center with any questions.

Don’t get hooked by phishing!

- Remember - Sharp will **never** ask you to divulge your password.
- Be alert – If you are being asked to enter credentials like usernames, passwords or credit card information in a website, be sure it’s legitimate.
- For more information, please visit: http://sharpnet.sharp.com/is/informationSecurity/index.cfm

Passwords

- Passwords are vital in connecting you to variety of systems and resources, including those storing employee and patient information.
- In order to stay secure, the usage and selection of your passwords are very important.
- Consider what could happen to you if a password to one of your personal websites was stolen.

Password Security in the News

"Hackers have stolen usernames and passwords for nearly two million accounts at Facebook, Google, Twitter, Yahoo and others, according to a report released this week."

"The massive data breach was a result of keylogging software maliciously installed on an untold number of computers around the world…The virus was capturing log-in credentials for key websites over the past month and sending those usernames and passwords to a server controlled by the hackers."

Source: http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/

Password Security

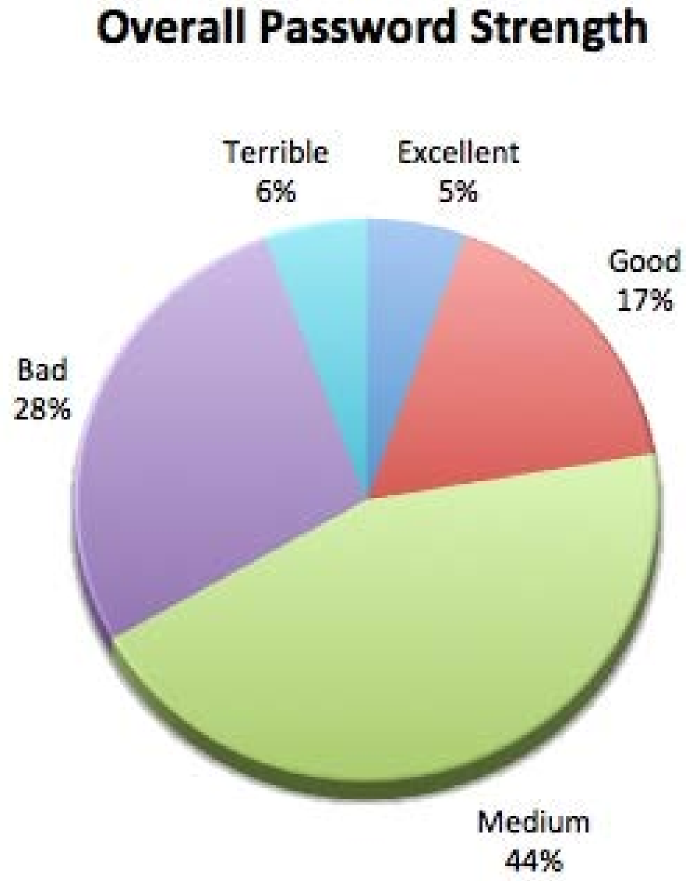
- What are some ways to reduce the risk if your password is stolen?
- Also, how can you choose a strong password for your different systems and websites?
- Please consider the following tips to protect yourself and your information.

Avoid Password Reuse

- In our personal lives, we use a different key to lock our house, office or car.
- As a result, if someone were steal a single key they wouldn't be able to break into everything.
- Just as you use a different key to protect your valuables, try using a different password for the websites or systems you use.
- If a password is stolen, it could potentially be reused on your other websites, unless you've used a different one.

Use a Strong Password

- Using a strong password also reduces the chances that it will be compromised by an attacker.
- Statistics from a recent website breach of over 2 million accounts show that many users choose weak passwords.
- Password strength for only 22% of the users were found to be either “strong” or “excellent”.



Source: http://blog.spiderlabs.com/2013/12/look-what-i-found-moar-pony.html

How to select a strong password

- Step 1: Join two unrelated words with a total of at least 8 upper and lower case alphabetic characters with numbers between them (e.g., **Ant32Scan**). This is your *base password*.

- Step 2: Take your *base password* and add a few additional characters that relate to each website:
  - Gm**Ant32Scan**ail! – for your Gmail account
  - Ch**Ant32Scan**asebank! – for your Chase banking account
  - Tw**Ant32Scan**eet! – for your Twitter account
  - Fa**Ant32Scan**cebook! – for your Facebook account

Congratulations! You have just created strong, yet memorable passwords that will be unique for each website you regularly use.

Note: Please do not use these sample passwords.

What to do if you believe your password has been stolen

- If you believe a password to one of your personal website accounts has been stolen, change it immediately.
- If you believe that the password to one of your Sharp accounts has been stolen, please contact the Help Desk/Technical Assistance Center at (858) 627-5000 to have it reset.

Personal Devices

- Personal devices play an important role in staying connected.
- In general, people are increasingly relying on their smartphones, tablets, laptops or other devices for work and other daily activities.

Personal Device Security

- Using personal devices to access sensitive information represents a risk to healthcare systems such as Sharp.
- If proper precautions are not taken to safeguard your device, it could potentially result in exposing sensitive information.
- What are some ways to reduce the risk of exposure when using a personal device?

Reducing personal device risks

- If you would like to use a personal mobile device to access Sharp resources, please get approval from your Senior Vice President and complete a Personal Device Agreement.
- This agreement can be downloaded from SharpNET at: http://sharpnet.sharp.com/webdocs/documents/policies/approved/13919_ATTACHA.pdf
- Please note that this may require the installation of Sharp supplied software to enforce Sharp's personal device requirements.

Additional Guidance

- Here are some additional tips to help secure your personal devices and minimize the risk of theft or loss:
  - Never leave your personal device unattended
  - Password-protect your personal device with a PIN.
  - Configure the lock screen feature to come on after a short period of inactivity.

If a personal device is lost or compromised…

- Please contact the Help Desk/Technical Assistance Center at (858) 627-5000 to determine if a security and/or privacy breach has occurred.
- For additional information regarding personal devices, please review Sharp policy #13919: http://sharpnet.sharp.com/webdocs/documents/policies/approved/13919.doc

Sensitive Information and the Web

- Since the Internet make its so easy to communicate, it is also easy to disclose sensitive information, including patient data.
- What steps can you take to ensure that sensitive information stays secure while using the Web?
- Please consider the following areas where good security decisions are needed to reduce risk.

Use of Cloud Services

- What are cloud services?
  - Cloud services use remote machines owned by another company to run everything from e-mail to complex data systems.
- Many cloud services are intended for personal information storage and sharing.
  - Examples include web-based services such as Dropbox, Gmail and Yahoo mail.
- When used for business purposes, cloud services introduce significant risk as shown in the following example…

Cloud Services in the News

- The Oregon Health & Science University has notified 3,044 patients that their protected health information has been compromised after several well-intentioned medical residents and physicians-in-training *inappropriately used Google cloud services* to maintain a spreadsheet of patient data.

Source: http://www.healthcareitnews.com/news/fourth-big-hipaa-breach-ohsu

Considerations for Cloud Services

- Although well-intentioned, the previous example shows how inappropriate usage of cloud services resulted in a reportable breach at another healthcare provider.
- So, how can you avoid the risks associated with cloud services?

Cloud Services Guidance

- Prior to any corporate usage of a cloud service, please first have it reviewed by Sharp Information Systems.
- To start the review process, please work through the appropriate IS Contact such as an IT Liaison or Manager.
- The IS Contact will then collaborate with the appropriate Sponsor for it to be reviewed by Sharp's Technology Review Committee.

Cloud Services Risk Assessment

- As part of the review, a risk assessment will also need to be performed by Sharp Information Security.
- For any questions related to the risk assessment process, please contact the Information Security Office at 858-499-6231.

Additional Guidance

- Please note that the storage of restricted data, which includes Protected Health Information (PHI), using cloud services that are not managed or otherwise explicitly approved by Sharp is prohibited.
- For further details of the review process, please reference Sharp’s Information Systems Technology Acquisition policy #13452.99:

http://sharpnet.sharp.com/webdocs/documents/policies/approved/13452.99.doc

Use of Social Media

- The use of social media is another area where caution is needed.
- If used inappropriately, it could expose sensitive information.
- Consider an example where the use of social media inadvertently exposed patient information.

Inappropriate exposure of patient information

- *[A doctor in Rhode Island] was fired from the hospital last year and reprimanded by the state medical board last week. The hospital took away her privileges to work in the emergency room for* ***posting information online*** *about a trauma patient.*
- *[The doctor's] posting did not include the patient's name, but* ***she wrote enough that others in the community could identify the patient****, according to a board filing.*

Source: http://www.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/

Social Media Guidance

- How can you avoid the risks associated with social media?
- Do not discuss individual patients, use PHI or anything that could be reasonably perceived as PHI.
    - Remember, the posting in the previous example did not include the patient's name, but there was *enough information* that others in the community could identify the patient.
- For further guidance on the use of social media, please review Sharp's social media policy #13522:

http://sharpnet.sharp.com/webdocs/documents/policies/approved/13522.doc

Staying Secure

- It is not always easy to maintain the balance of being connected and staying secure.
- Sharp wants to you make good decisions in this connected world
  - Watch out for phishing
  - Avoid password reuse
  - Use personal devices and the web responsibly
- By making good choices, you can stay productive and remain secure!

Exit Instructions

We hope this course has been informative and helpful.

Please take the

Module 4 Quiz