Understanding Security Threats in the Cyber World

Beth Chancellor, Chief Information Security Officer
• Phishing
• Credit Card Fraud & Identity Theft
• Cloud Services
• Social Networking
• Wireless
An attempt to deceive users into giving out personal or other confidential information.

- Phishing is typically conducted via email, sometimes over the phone. In all cases, social engineering is at play
- There are many versions of Phishing (Phishing, Whale Phishing, Spear Phishing, Smishing, etc.)
- Legitimate companies and organizations do not send unsolicited emails requesting personal information, account information or passwords.
Email Spoofing –
   - Emails that look like they are coming from a legitimate email address but are really from someone else.

Account Compromises –
   - Email accounts are often compromised and used to solicit information and money.
Advice

• Do not reply to emails that ask for personal information, account information or passwords.
• Be suspicious of any email with urgent requests for personal or financial information.
• Report phishing attempts
• If you get a phone call asking for personal information, call them back at a number you find on your own.
Phishing

Advice

• Do not use the links provided in an email to get to web pages if you suspect the message might not be authentic.
• Only use web sites that you browse to on your own.
• Don’t fall for the “I’m on vacation and lost my wallet” trick
ST. LOUIS (KSDK) - The Schnuck’s credit card breach impacted about 2.4 million credit and debit cards used at 79 of its 100 stores, according to the company.

The company said the breach happened over a three month period, between December 2012 and March 29, 2013.

BOSTON (AP) — A hacker or hackers stole data from at least 45.7 million credit and debit cards of shoppers at off-price retailers including T.J. Maxx and Marshalls in a case believed to be the largest such breach of consumer information.
Credit Card Fraud and Identity Theft

Advice

• Check your bank and credit card statements regularly to ensure that all transactions are legitimate.

• Check your credit rating often.

• Sign-up for credit monitoring and/or identity protection services
Credit Card Fraud and Identity Theft

Advice

• Always ensure that you are using a secure website when submitting credit card or other sensitive information via the web. Look for **https** in the url.

• Make sure you have fraud protection through your bank or credit card company.

• Be careful when signing up for things like “my Panera card” or other “rewards” cards.
• A service or application that is:
  – Internet delivered
  – Owned and controlled by another person or organization
  – Location of data storage is unknown
  – Typically free (but not always)
Cloud Services

Examples

• iCloud (Apple)
• SkyDrive (Microsoft)
• Mozy
• Google Drive
• Google Apps
• DropBox

Interesting thing about consumer cloud services. You have to agree to their terms but they usually don’t have to agree to any terms for your benefit.
Dropbox gets hacked ... Again

After last year's embarrassing data breaches, Dropbox promised to implement additional safeguards "to prevent this from happening again." Whoops, it just happened again.

By Ed Bott for The Ed Bott Report | August 1, 2012 -- 01:47 GMT (18:47 PDT)
Cloud Services

Risks and Issues

• Service availability

• Consumer-based services are not secure
  – Cloud email is not encrypted
  – Services are prone to being hacked.
    • because they aren’t as secure as they should be
    • because they are targets

• Cloud providers don’t always tell people when they get hacked

• No delegate rights for account access
  – Cloud providers will not give access to anyone other than the account holder unless it’s through a legal process like a subpoena. (This is different than how we deal with access at work)
Advice

• **Think twice** about storing sensitive information such as copies of social security cards, social security numbers, tax returns, credit card numbers, bank account numbers, personal information about you or your family, in the cloud.

• Contrary to what we tell you at work, you should probably share (or store somewhere) login IDs and passwords with someone you trust.

• **Don’t send confidential information**, such as credit card numbers, SSNs, etc., in via email.

• If you must send sensitive information, **put it in a document and password protect the document** or better yet, call the person you are dealing with.
Social Networking

• Information posted to a social networking site or service is no longer private
• Social engineering is active on social networking sites
• Sites/services are hackable
  – There are a multitude of tools and techniques available that help people hack accounts
  – April 23, 2013 - AP Twitter account hacked, makes false claim of explosions at White House
Advice

• Don’t over share - Once on the Internet, it’s hard to make it go away
• The more you share the more likely you can be impersonated
• Understand and use the security tools available on social networking sites
• Don’t “friend” people you don’t know.
• Monitor your kids’ use - Children are easily tricked or exploited
Various forms of wireless technologies

- Bluetooth
- Wifi
- Mifi
- Cellular wireless (3G, 4G, etc.)
- Cellular wireless modems

Wireless hacking tools and applications do exist
Advice

• Turn off all wireless connections (WiFi and Bluetooth) when not in use
  – Maintains security and saves battery life
• Don’t use unsecure WiFi. If you must use it, only use it for pure browsing
• Cellular wireless (your data plan) is considered secure
Wireless

- Unsecure WiFi
- Be sure to secure your home WiFi
- Change the default password
Consider encrypting your devices if technically possible

- Encryption protects data on your computer/devices if it’s lost or stolen.
- Variety of consumer oriented encryption software is available (Bit Locker, File Vault, TrueCrypt, etc.)
- Use encryption tools for accounts and passwords (such as KeePass)
Other Tools

Set up built-in tools like
- Find my iPhone
- Device wipe if the wrong password is used x times

Antivirus
- Make sure you have and maintain antivirus software
- Run antivirus scanning on a scheduled or frequent basis
- Keep Operating systems up to date
- Keep your phone operating system up to date
Other Tools

- Keep your computer firewall turned on.
- Don’t plug in USB drives from an unknown person or source, unless your antivirus software can scan it first (even then, you should think twice)
App Stores

• iTunes store applications are generally considered secure
• Other app stores are not necessarily secure
• Research apps before you buy them
• Keep apps updated. Updates often include security enhancements.
3 National Credit reporting companies
  – Experian
  – Equifax
  – TransUnion

Credit monitoring service (UM Benefits)
http://www.umsystem.edu/totalrewards/benefits/credit

Life Lock (as little as $10 per month)
www.Lifelock.com
Resources

FBI site about Social Networking Risks

FBI site about common scams
http://www.fbi.gov/scams-safety/fraud

MU Information Security Educational Resources
http://makeitsafe.missouri.edu

FCC site for Consumers
http://reboot.fcc.gov/privacy-and-online-security

Internet filtering software
http://www1.k9webprotection.com/
Questions?

Beth Chancellor
chancellorb@missouri.edu
573-882-3503