Tech Talk - Digital Security Reality Check

October 18, 2011

Roger Safian
r-safian@northwestern.edu
Agenda

• Why should you care about security?
• Passwords
• Mobile Devices
• Computers
• Social Networks
• Browsing
• E-mail & messaging
• Questions
On the Internet,
Nobody Knows You're a Dog

"On the Internet, nobody knows you're a dog."

• July 5th 1993
'I thought it was my sister': Woman loses $2,000 to Facebook scam

By Bob Sullivan

Now, you can't even trust your sister on Facebook.

Edythe Schumacher logged onto the social networking site recently and a picture of her sister popped up immediately, inviting her into a Facebook chat. After a bit of small talk, Schumacher's sister — Susan Palmer — egged her on to apply for a government grant, saying she'd just received one. For an up-front fee of $2,000, Schumacher was assured, she'd get access to up to $500,000.

Schumacher trusted her sister — and lost $2,000.
Reality Check

• One password is safe for all systems
  – Reality
  • A variety of passwords will protect you better
    – It limits damage if one is exposed
  • Your password protects more than your e-mail
    – Think about your reputation, or others who rely on your trust
Passwords

• Chose a password based on what you want to protect
• Never save your password in an application
  – Especially financial applications
• Don’t use the same password on a service as the e-mail account linked with that service
  – Amazon/e-mail == different passwords
• Change passwords when you think there is a problem
• Choose strong passphrases
  – Longer is better
    • Ilikeusinglongpasswords!
• Consider using a password vault
  – http://keepass.info/
    • Bonus – You don’t need to type passwords
One possible password system

• Choose three unique passwords
  – Casual with no important data
    • Example – newspapers
  – Important but no credit card data
    • Example – e-mail, social networks
      – You might want a unique password for your main e-mail account
  – Sites with credit card or financial data
    • Example – Amazon, iTunes
• Financial institutions should have their own unique password
Reality Check

• I only visit safe Web sites
  – Reality
    • You can get malware from legitimate web-sites
    • It’s difficult to recognize a hostile URL from one that is safe
    • Are you sure the links on your “safe” web-site are themselves safe?
Browsing

• Use the most recent version of your favorite browser
• Keep current with updates
  – Don’t forget add-ons
• Enable built in security features
  – Pop-up blockers & phishing filters
Browsing (cont.)

• Don’t trust pop-up messages
• Don’t assume that Google results are malware free
• Be careful when clicking on links
  – Use caution with shortened URLs
• Use “Favorites” for your regular sites
  – Especially for sites with a password
• Use Web of Trust
  – http://www.mywot.com/
Computers (Laptops, Desktops, Netbooks)

- Keep anti-viral software current
- Apply updates when available
  - Don’t forget installed software
    - Watch out for additional software when updating
- Remove old software
- If possible encrypt sensitive data
- Backup your data
  - Consider an off site solution
Reality Check

• Social networks are all about fun, I don’t need to worry about security
  – Reality
    • Even if you use them just for fun, others may not.
      – Businesses also use them
Social Networks (Facebook, etc.)

• Check before entering password
• Don’t share:
  – Address
  – Phone Number
  – Birthdate
    • Never the year if you give the exact date
  – E-mail address?
• Be careful when clicking on links
Social Networks (cont.)

• Give some thought to what you post
  – Just assume everyone will read it
• Think before accepting a new friend
  – How did this person find me?
• Don’t post the answers to your security questions
• Get further tips from online guides
  – Google “Facebook privacy guide”
Social Networks (cont.)

“If you are not paying for it, you’re not the customer; you’re the product being sold”

Think about this the next time you sign up for a “free” service
Reality Check

• I don’t care if someone else reads my e-mail
  – Reality
    • Would you care if they changed your direct deposit to go to their bank?
      – Your NetID is your key to a variety of university services.
E-mail & Messaging

- Don’t automatically trust messages
  - From: addresses are easy to forge
  - Malware often uses contact lists
- Never give anyone your password
- Use caution when opening attachments
- Double check links
Mobile Devices (Phones, PDAs)

• Enable a PIN and/or Autolock code
• Check for updates regularly
• Don’t automatically trust the app store
• Be cautious with
  – Apps
  – Links
  – Unknown Phone Numbers
• [Website Link](http://www.it.northwestern.edu/policies/mobile-devices.html)
Mobile Devices (Phones, PDAs) (cont.)

- Be careful with QR codes
  - Never scan a code by itself
- Don’t forget to update your apps
- If you do not use a feature, disable it
  - Bluetooth
  - 4g
  - GPS
  - Wireless
Online Resources

NUIIT Web info

• Computer and Network Security
  – http://www.it.northwestern.edu/security/index.html

• Reporting a Security Incident
  – http://www.it.northwestern.edu/security/help.html

• Secure the Work Environment
  – http://www.it.northwestern.edu/security/working.html

• Incident Response Protocol
  – http://www.it.northwestern.edu/policies/incident.html
• Roger Safian  
  – (847) 467-6437  
  – security@northwestern.edu  
  – r-safian@northwestern.edu  

• NUIIT Support Center  
  – (847) 491-HELP (4357)  
  – consultant@northwestern.edu
Questions?