Northwestern IT Tech Talk

Top 5 Tools for Securing Your Devices

Mary Carp
Data Security Analyst
Northwestern Information Technology
Information and Systems Security/Compliance

May 19, 2016
Antimalware
Antimalware

• What is malware?
  – Viruses, Trojans, worms, adware, spyware, etc.
  – A rose by any other name…is still malicious software
  – Most major “antivirus” programs tackle all of it
Antimalware

• Common Attack Vectors
  – E-mail attachments
  – Software downloads
  – Transfer from another infected device
  – Drive-by downloads

• Applicable on all devices
Antimalware
Antimalware

• Common Attack Vectors
  – E-mail attachments
  – Software downloads
  – Transfer from another infected device
  – Drive-by downloads

• Applicable on all devices
Antimalware

• Before you download, ask yourself:
  – Do I trust the author of the content?
  – Do I trust the website/host of the content?
  – Do I understand what this application is supposed to do?

• But even so…
  – INSTALL ANTIMALWARE
Antimalware

• Antivirus Options
  – University-owned machines: Symantec (NU license)
  – Personally owned machines: Symantec (NU license), Windows Defender, Avast, Malwarebytes, AVG, etc.
  – Mobile devices: Lookout, Avast, etc.
  – Take care when downloading free antivirus software/apps

Northwestern antivirus options
Antimalware
Antimalware

• Antivirus Options
  – University-owned machines: Symantec (NU license)
  – Personal machines: Symantec (NU license), Windows Defender, Avast, Malwarebytes, AVG, etc.
  – Mobile devices: Lookout, Avast, etc.
  – Take care when downloading free antivirus software/apps
Antimalware

• Adblockers/plugins
  – E.g. AdBlock Plus
  – Take care when downloading adblocking plugins
  – Be sure to add exceptions for pages that you trust
Backup Utilities
Backups

• Backup Utility Options
  – University Data: CrashPlan
    • Hon. Mention: Box, SharePoint
  – Personal Data:
    • Local backups – Time Machine, Windows Backup and Recovery, etc. to external hard drives, flash drives, CDs/DVDs
    • Cloud backups – Google Drive, DropBox, iCloud, etc.
## Backups

<table>
<thead>
<tr>
<th>Data Type &amp; Examples</th>
<th>SharePoint</th>
<th>Vault (Research Only)</th>
<th>Northwestern Box</th>
<th>Northwestern File Servers</th>
<th>Google @u (Student Collaboration)</th>
</tr>
</thead>
</table>
| **Public**
(e.g. calendar, course descriptions, maps, directory, approved census facts, audited financials) | No         | Yes                    | Yes              | Yes                       | Yes                              |
| **Internal: Non-Sensitive**
(e.g. meeting agendas, project documents, team building event) | Yes        | Yes                    | Yes              | Yes                       | Yes                              |
| **Internal: Sensitive**
(e.g. salary plans, employment data, budgets, donor information, IRB data, CTEC, patent information) | Yes        | No                     | No               | Yes                       | No                               |
| **Legally/Contractually Restricted**
(e.g. PHI, SSN, PII, student records, medical records) | Yes        | No                     | No               | Yes                       | No                               |

### File sharing at Northwestern
Backups

• Backup Utility Options
  – University Data: CrashPlan
    • Hon. Mention: Box, SharePoint
  – Personal Data:
    • Local backups – Time Machine, Windows Backup and Recovery, etc. to external hard drives, flash drives, CDs/DVDs
    • Cloud backups – Google Drive, DropBox, iCloud, etc.
Backups

• Backup Strategy
  – What do I need to back up?
    • How much backup space do I have?
    • What data is already backed up in the cloud? E.g. music purchases
  – How often do I need to back it up?
    • How many versions can I lose?
  – Where should I back it up?
    • How sensitive is my data?
    • How likely is my backup to suffer the same failure as the original?
  – How long should I keep the backups?
    • What are the legal retention requirements?
    • What are my personal retention requirements?
Encryption Software
Encryption

Before

This is regular text. When it is encrypted it cannot be read without the password that was used to encrypt it. You can copy and paste information here from other programs and encrypt it. For example, if you wanted to encrypt an email message you could copy the email contents here, encrypt it, paste it back into your email program, and then send an encrypted message.

After

hQHOA3TgMYCtjErAEAb+ILsA41Phxl/SfqdocLgwM85EzaNReo+Pu65+IyYc6wiD
oeh2pchGY4M5GD0Vo9aFwS08fT3jSxf6neqZTJID60cpZIlg10DF+TqeMlavYlB
XwtnEOI+iXH6QHqY0hZbxERwRSyrqxBq1PSazwJqq87nob39XUlK/xleWcyf/NoYw6
Xi858NNO1Enntv000Ch6RMmdez6E73z/lop+VKh0AnivGEuluhorTcW/GqnjdzmA
dy61UX4LKD02OjxmcPdt50oxX+E+2ukSZhSrVDfUev8IbuYFL8Du4Z2DTuHBjhrM0G
/251pgUSi0+NHuykVKeWdhem/QD2aRxkfn4Ek4Pr4zqC24PZXYOW+CdVZmwR93
PCpENVkhxV0rqJJi48H1NEeohjLfuUy09mE8yPnKVTn7ThUoF99eKaxUhz1LQ
Y5t3yqrJ6JmdVJSkINLYygeIFmapJupIbcwpN5sV//p0ld3qvy0VCY/bD1+egTmnz4F
HrzQnkZxNtULB7Z03mE+/M3Kso+7FSMsbmwpMlnRIwGhGnNpblz/mkdTSXv507
BGR7g9JwjbavouQMQR1Ob6cspr9nr+6l902JiOzZ0/SY0sAASQ+5v7/1CF+khY+
YKfJgGguems+MfiyLv4WBH7UeJUkgDJ6nW9lXjr+trSih1YmmhOmToyYuGwsYAfQ
fhz4hhtf+2MuXq+KMyyAfofsRqgd2i2nvu88&Z2Aji+BfQN5qY}VYoW/IMmUZNjM
FszlwD7Kk+ZYdTt2/MIQGhpj0L1aky53nnugYU6wxqn5Z2SZd5Sax7DDeQBHfVK
Rb+Gxl/emo/yFl+/DY11qbtNU1sntoIJC7GhKHYTHPObKnx6m+HN2vndhYIAUG74
+WRp3KIweh8Fj2JEa8Z493zQad6YgLAcjKJQGY1Urd/X
=G+X8
Encryption

• Full-disk Encryption
  – Encryption of entire drives
  – Good for laptops/mobile devices
  – Microsoft Bitlocker, FileVault2 for Mac

• File-level Encryption
  – Encryption of specific files or folders
  – Good for shared stationary computers
  – PGP, Truecrypt
Encryption

• Network Encryption
  – Encryption of data as it moves across a network
  – Often performed for you via your browser
  – VPNs and other secure tunnels

Northwestern VPN
Encryption

• File Shredding
  – Secure Empty Trash on Mac
  – Eraser, PGP on Windows
Encryption

• BE EXTREMELY CAREFUL WITH THIS TOOL
  – Back up recovery key
  – Back up the backup of your recovery key and save it somewhere else
  – Back up your data—unencrypted—in a secure location
  – Do not encrypt University-owned devices without the assistance of your local IT staff
Multifactor Authentication
MFA

• Methods of authentication
  – Something you have (a key, a USB stick, etc.)
  – Something you are (fingerprints, retinas, etc.)
  – Something you know (password, PIN, etc.)

• Some of these are easier to compromise than others

• MFA uses multiple methods of authentication to provide defense in depth
MFA

• **MFA at Northwestern**
  – Duo Security
  – NetID AND
    • Phone call to a line of your choice OR
    • Push notification to your smartphone
  – Required for Direct Deposit
  – Expect to see more systems behind MFA in the future
MFA

• Other resources with optional MFA:
  – Gmail, Yahoo, Hotmail
  – AppleID, Microsoft account
  – Facebook, Amazon

• Banking sites often require MFA

• Duo can be used for many of these, but they provide additional MFA options as well, including phone calls, emails, and other apps
MFA

• Multifactor authentication makes it exponentially harder to compromise an account

• As technology progresses, passwords will become more and more difficult to secure: MFA is the future of authentication
MFA

MULTIFACTOR AUTHENTICATION

IS COMING
Password Manager
Password Mgmt

• Passwords should not be stored:
  – On sticky notes under your keyboard
  – In an unsent text message to yourself on your phone
  – In a Word or Excel document on your computer
  – In your significant other’s brain
  – In plaintext, anywhere
Password Mgmt

• Password Managers
  – Encrypted databases for storing credentials
  – Cross-platform local options (KeePass, Password Safe, etc.)
  – Cloud-based options (LastPass, etc.)
  – Preferably secured with MFA
Password Mgmt

• Benefits
  – Can store other relevant information: security questions, URLs, notes, etc.
  – Only need to remember one password
  – Can generate passwords
  – Can copy credentials without viewing and clear clipboard after a short interval
  – Makes it reasonable to use truly variant passwords
Password Mgmt
Password Mgmt
Wrap-Up
Summary

• Step 1: Security Awareness
• Step 2: Security Tools
• Step 3: Profit
Secure IT @ NU

- Computer and Network Security
  - [www.it.northwestern.edu/security/](http://www.it.northwestern.edu/security/)
- Information Security News Podcasts
  - [www.it.northwestern.edu/security/podcast.html](http://www.it.northwestern.edu/security/podcast.html)
Contact Information

• Mary Carp
  – (847) 467-5996
  – m-carp@northwestern.edu
  – security@northwestern.edu

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