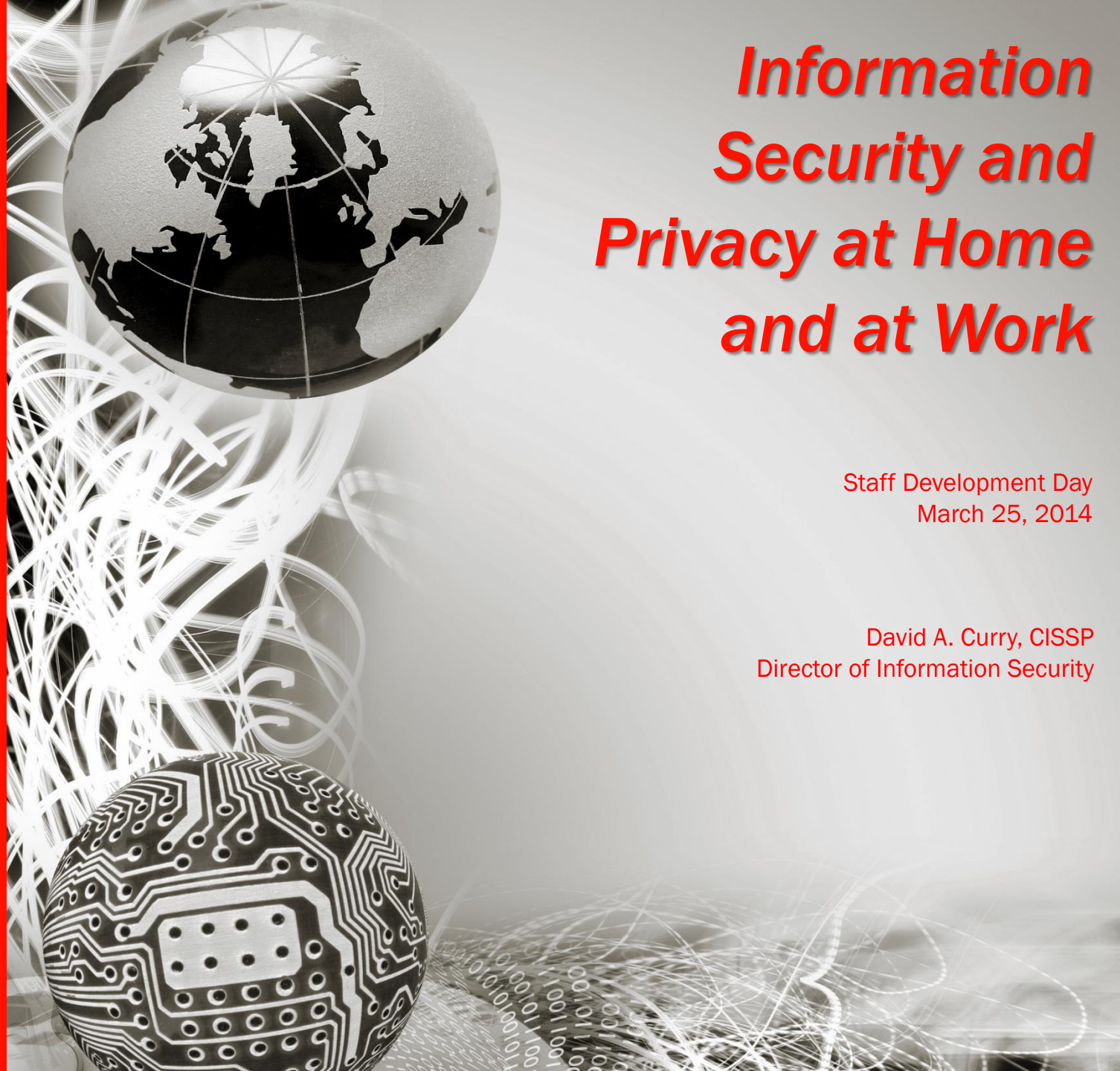
THE NEW SCHOOL



Information Security and Privacy at Home and at Work

Staff Development Day
March 25, 2014

David A. Curry, CISSP
Director of Information Security

Always start with some definitions…

- Information Security
  - **Confidentiality** – making sure that information is accessible only by individuals who have been authorized to access it; ensuring that information is never disclosed to unauthorized persons
  - **Integrity** – safeguarding accuracy and completeness of information and information processing methods; preventing unauthorized changes to information
  - **Availability** – ensuring that authorized users can access information in a timely manner, when it is needed; making sure that information systems are up and running when they should be
- Information Privacy
  - The interest an individual has in controlling, or at least significantly influencing, how data about him/herself is collected, used, shared, kept up-to-date, and disposed of

Security and privacy at The New School

- Information Security Policy
- Information Resource Acceptable Use Policy
- General Controls for Handling Sensitive Information
- Desktop Information Security Guide
- IT Web Site

Securing your computer and home network

- Keep your operating system up-to-date
  - Configure Windows Update to “Install updates automatically” and “Include recommended updates”
  - Configure Apple Software Update to “Check for updates daily” and “download updates in the background”
  - When prompted to install updates, **install them!**
- Keep applications up-to-date
  - If an application can check for and/or install updates automatically, or at start-up, enable that feature
  - On Windows, consider using Secunia Personal Security Inspector or FileHippo to periodically check for application updates
  - On Macs, consider using AppFresh or MacUpdate Desktop to check for application updates
  - When updates become available, **install them!**

Securing your computer and home network (cont'd)

- Run an up-to-date anti-virus / anti-malware program
  - Free or commercial, take your pick – stick with well-known brands
  - Yes, this applies on Macs too
- Enable (don't disable) your operating system's firewall
  - If anti-virus / anti-malware product wants to disable it that's okay
  - Otherwise, don't touch it
- Change the password on your router
  - Home routers / switches / Wi-Fi access points ship with well-known admin passwords
- Put a password on your Wi-Fi
  - Enable encryption:
    - WPA2 is better than WPA is better than WEP is better than nothing

Keeping information safe and secure

- Protect your passwords
  - Use only strong passwords
    - Minimum 8 characters, mixed case, digits, special characters
    - Pass phrases are even better (but avoid “common” phrases)
  - Use different passwords for different sites
    - Separate work and home, finance and social networking, etc.
    - Use a “template” approach to keep them straight if you want
    - Avoid social network logins for “important” sites
  - Don’t save passwords or write them down
    - Built-in web browser “save this password” features are **not** secure
    - Do not store them in a spreadsheet, write them on a Post-it, etc.
  - Use a password manager
    - Keeps all passwords safely encrypted, automatically generates good passwords, lets you access passwords from anywhere, etc.
    - LastPass, KeePass, 1Password, others

Keeping information safe and secure (cont'd)

- Regularly back up your data
  - New School information
    - New School information should be backed up to departmental share drives (preferred) or removable media
    - Google Drive/Docs should not be used to store "master" copies of business records
    - Use of cloud-based backup solutions is **not acceptable**
    - Desktop computer hard drives are **not** backed up
  - Personal information
    - External hard drives are okay, but do not remove risk of damage by fire or flood or loss due to theft
    - Removable media can be stored in a remote location (but make sure it's a secure location)
    - Cloud-based services are probably the best option
      - Mozy, Carbonite, Dropbox, iCloud, Google, etc.

Keeping information safe and secure (cont'd)

- Securely destroy obsolete information
  - New School information
    - Paper containing Restricted or Confidential information should be shredded (cross-cut or micro-cut) or placed in secure (locked) bins
    - CD-ROMs and DVD-ROMs should be shredded or broken by hand
    - Hard drives and tape media should be returned to IT for secure disposal
  - Personal information
    - Paper should be shredded with a cross-cut or micro-cut shredder
    - Hard drives should be removed from old computers and destroyed
    - CD-ROMs and DVD-ROMs should be shredded or broken by hand
    - USB flash drives can be smashed with a hammer
- Lock your screen when you leave your desk
- Use a locking screen saver

Personally identifiable information (PII)

- Name
- Address(es)
- Telephone number(s)
- Date of birth
- Place of birth
- Social Security number
- Other identification numbers
- Gender and gender identity
- Marital status
- Family
- Education
- Religion
- Beliefs (political, etc.)
- Profession
- Criminal record
- Financial information
- Medical information
- Biometric information (fingerprints, retinal scans, genetic information)
- Other indirect identifiers (mother's maiden name, etc.)

- Fun with "big data"
  - 87.1% of people in the United States can be uniquely identified using only 5-digit ZIP code, birth date, and gender (Sweeney)
    - 53% by *city*, date of birth, and gender
    - 18% by *county*, date of birth, and gender
  - First 5 digits of SSN can be correctly predicted 61% of the time using only date of birth and state of birth (Acquisti & Gross)

Guarding your personal information

- Watch out for phishing scams
  - **Always** be suspicious of emails asking for sensitive information
  - **Never** respond to an email request for personal information
  - **Never** click on the links in a suspicious email

  The TNS IT Help Desk will never ask you to provide or confirm personal or account information via email/clicking a link/filling out a form
- Sending personal information via email
  - Avoid doing this whenever you can -- enter via web site, fax, phone
  - If you can't avoid it, try to find a way to encrypt the information
- Sharing information in social media
  - Know who you're sharing with – limit things to "friends" or "circles"
  - Remove geo-tagging information from photographs you share
  - Don't let mobile apps share your location
  - Don't "check in" to locations publicly

Guarding your personal information

- Identity theft
  - Monitor your bank account and card transactions and balances
    - Set up automatic alerts if your bank / card provider offers them
  - Monitor your credit report
    - Get free (really free) credit reports from AnnualCreditReport.com
    - Credit monitoring services are, generally, not very useful (Krebs)
  - Monitor your health insurance
    - Read explanation of benefits statements carefully
- Stopping annoyances
  - National Do Not Call Registry: DoNotCall.gov
  - Pre-screened Credit Card Opt-Out: PreScreenOptOut.com
  - Junk Mail (Direct Marketing) Opt-Out: DMAChoice.org

Mobile device security

- Don’t store confidential information on your device
  - At the very least, keep it encrypted
- Keep software official and up-to-date
  - Install the latest operating system
  - Be sure to update apps regularly
  - Only use official app stores
- Back it up
  - Keep things in the cloud as much as possible
  - Enable automatic sync (most let you restrict it to wi-fi only)
- Set a PIN, password, or pattern
  - Set device to auto-lock after a couple of minutes
  - Avoid obvious PINs, passwords, and patterns

Mobile device security (cont'd)

- Be careful what you keep in text messages
  - Delete personally identifiable information and security information
- Turn off Bluetooth if not in use
  - Bluetooth can be used to steal information from your device
- Know your Wi-Fi access point
  - Make sure you know the network you're connecting to
    - Just because it says "starbucks" doesn't mean it's Starbucks
  - Disable "connect automatically" for rarely-used networks
- Lock it up
  - Keep phones and tablets out of sight
  - Use a locking cable with your laptop
  - Put it in the trunk, not the back seat

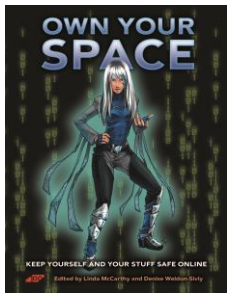
Safeguarding kids on the Internet

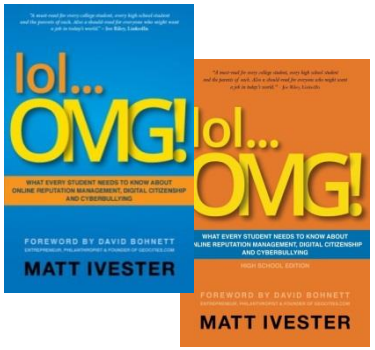
- Keep computers used by children in an open family area – never in their bedroom or the basement
- Screen names, accounts, and passwords
  - For children and young teens, parents should know all of them
  - Make sure they don't reveal full name, age, hometown, school
  - Young children should share a family email address rather than having their own accounts
  - Register children on on-line sites using parent's email address
- Make sure your kids understand that once you post it, you can't take it back
  - Teens have a hard time envisioning the future – how a post they create today may come back to haunt them when applying for college or a job

Safeguarding kids on the Internet (cont'd)

- Explain to kids the dangers of sharing personal information on-line
  - Anyone can see public posts: friends, neighbors, teachers, pastors, law enforcement, college admissions counselors, future employers, strangers, …
  - Use built-in controls on Facebook, Google+, Instagram, etc. to limit posts to friends
  - Never post full names, addresses, phone numbers, bank accounts, or credit card numbers
  - Don't publicly post the name of their school, favorite sports team, where they work or hang out, or friends' names – child predators are clever when it comes to physically locating teens
- Warn kids about flirting with strangers online
  - Make sure they know to come to you if they are suspicious or feel threatened

Safeguarding kids on the Internet (cont'd)





- OnGuard Online (web site)
  - Computer security, online safety for kids, avoiding scams, etc.
- Own Your Space (free download)
  - Aimed primarily at pre-college teens
  - Covers security, privacy, bullying, social media
  - Dated in spots but advice still applies
- lol…OMG! (Amazon, etc.)
  - Aimed primarily at college and high school students
  - Covers social media – how to use it safely and how to get in trouble
  - What to do about cyber bullying

Resources for further information

- New School IT Security Web Site
  - http://www.newschool.edu/information-technology/security
  - Policies and Standards: data classification, handling sensitive information, and more
  - Security Handbook: detailed information, including how-to instructions, on securing your computer and information
  - Copies of the Desktop Information Security Guide and this presentation (on the “Security Handbook” page)
- OnGuard Online
  - http://www.onguardonline.gov/
- “Own Your Space” download
  - http://www.ownyourspace.net/

Resources for further information (cont'd)

- Free credit reports
  - https://www.annualcreditreport.com
- National Do Not Call Registry
  - https://www.donotcall.gov/
- Pre-screened credit opt-out
  - https://www.optoutprescreen.com/
- Junk mail opt-out
  - https://www.dmachoice.org/

References

- Acquisti, Allesandro & Gross, Ralph. “Predicting Social Security Numbers From Public Data”
  - http://www.pnas.org/content/106/27/10975.full
- Krebs, Brian. “Are Credit Monitoring Services Worth It?”
  - http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/
- Sweeney, Latanya. “Simple Demographics Often Identify People Uniquely”
  - http://dataprivacylab.org/projects/identifiability/index.html

Questions