Protecting your Data, Devices, and Digital Life in a BYOD World: A Security Primer

GLENDA ROTVOLD AND SANDY BRAATHEN

NBEA

APRIL 2, 2015

What are You Trying to Protect?

- If someone got into your email, what information could they collect or retrieve and what could they do with that?
- Online browsing history, preferences?
- Credit card information?
- Personal information?
- Financial information?
- How much risk are you willing to accept?

Mat Honan's Epic Hack

- Could easily happen to any of us!
  - Digital life destroyed in 1 hour
    - Google account deleted
    - Twitter account compromised
    - AppleID account broken into,
    - Remotely erased all data on iPhone, iPad, and MacBook—more than 1 year's data, emails, family pictures)

Epic Hack
Sequence of Events

- 4:33 hacker called for password reset claiming to be victim. Received temporary password
- 4:50 password reset confirmation arrived in inbox with link to permanently reset AppleID password
- 4:52 Google password changed
- 5:02 Twitter password reset
- 5:00 used iCloud's "Find My" tool to remotely wipe iPhone
- 5:01 wiped iPad
- 5:05 wiped MacBook, deleted Google account
- At this point, they had total control to account and able to prevent victim from regaining access to account

Take Aways to Protect Your Digital Life:

- Use different passwords for accounts
- Backups! Backups! Backups!
- Consider using multi-factor authentication

Passwords

- Use strong passwords (combination of upper case and lower case letters, numbers, and possibly special characters
- Password strength (affected by number of characters possible and the length, x^y)
- Change frequently
- Use different passwords for different accounts
- Do not share passwords; store in safe location
- Password-protect your computers and notebook; consider password protecting certain files
- Use passcodes (consider longer vs. simple PIN) on mobile devices

Backup, Backup, Backup

- Backup—Make a copy of files in another location
  - Thumb drives
  - External hard drive
  - Cloud Storage
- Backup regularly

2FA—Two-Factor Authentication (Multi-factor authentication

- Two-Factor Authentication—using multiple methods to prove you really are who you say you are
  - Something you know—passphrase, PIN, password, code
  - Something you have—physical token, chip, fob, phone
  - Something you are—biometric (ex: fingerprint)
- SMS two factor authentication
  - Your phone is a second factor authentication device via code texted to the phone
  - OTP (one-time password) sent to phone

Setting up 2FA

- Set up two-factor authentication on popular social networking sites and platforms:
  - Facebook, Twitter
  - Apple
  - Google, Microsoft Outlook, Yahoo!
  - Dropbox
  - LinkedIn
  - Ebay/PayPal, Evernote
  - http://stopthinkconnect.org/2stepsahead/how-to-enable-2-step-authentication/
- When setting up 2FA or use of security questions on business accounts (such as banking) or other accounts:
  - Do not select questions that can be answered by doing an Internet search; or if you do, then give a fake answer.

Other Security Terms

- Encryption
  - Encodes data so that it is undecipherable
  - Can be applied to data at rest (stored on disk) or in transit (wireless—WPA/WPA2, https, vpn, etc.)
  - Unencrypted data can be sniffed (captured) with Packet Sniffing software
- VPN (Virtual Private Network)
  - Connect with a VPN client to corporate or through VPN service provider
- Pen testing (Penetration testing)
  - Using software tools or other strategies to see if one can hack into or gain unauthorized entry into a system
- Brute Force Password attack

Security Precautions

- Consider using a VPN at public wi-fi spots or to connect to public APs (access point)
- Ignore password request e-mails or security alerts on smartphone (high probability of being fraudulent)
- Consider installing security scanner app on phone/iPad/tablet to see if device is uploading private data to cyberspace
- Consider installing other security apps (including anti-virus)
- Don't use third-party apps or jail-break phone
- Update devices with latest OS updates and browser updates
- Read security notices when installing apps (especially Android) to see how sensitive data may be exposed
- Disable GPS as needed; don't give home address on map apps; remove GPS/location data from pictures before posting

(Siciliano, 2014)

Security Precautions (cont.)

- Don't give your real birthday on sites
- Don't post too much information on social networking sites
- Don't use any information posted on sites as the answer to a security question, a password, etc.
- Don't use words, names, sequential numbers, etc. as passwords. A brute force attack could crack your password.
- When you don't need to be on the Internet, go offline
- Don't keep apps open and logged in
- Don't save login names and passwords in your browser
- Use Private Browsing feature (especially on public computers)

Protecting your Data

- Adopt a proactive security mindset
  - Think like a hacker!
- Limit private data stored on phone for long periods of time
  - Worst case scenario—what can you afford to lose?
- Backup data, pictures, attachments to other location
- Treat smartphone like your regular computer (your phone is a computer too!!)
- If Bluetooth is enabled, disable "Discoverable" setting
- Use encryption (varies by device, built-in or 3rd party)
- Change highly sensitive app icons and labels to something unrelated or something perceived as useless

Protecting Your Data

- Protecting credit card information
  - Use cash
  - Use https when online
  - Use virtual credit card numbers
- Don't sign up for new service using a social networking account
- Lock down social media profiles

(Mitchell, 2014)

Research Apps Before Downloading

- Some apps ask for permissions; some permissions can subject user to unwanted risks (ex: capture conversations, pictures, turn on your camera, record screen images of personal data being entered)
- Research the app's ratings and reviews
- Download only from trusted app stores
- Read the Terms of Service to determine what data on your phone/device will be accessed

Siciliano, 2012

Consumer Reports Nationwide Survey Results

- 34% of all smartphone users do not use any form of security for their mobile device
- Only 36% use 4-digit pin to lock their phone
- Only 22 percent install software to find the phone
- Only 14 percent install antivirus app
- Only 11 percent use pin longer than 4 digits
- Only 8 percent install software that can erase data
- Only 7 percent use *other* security features (ex: encryption)
- Estimates over 4 million smartphones were lost or stolen last year

General Smartphone /Mobile Device Security Recommendations

- Physically protect devices and keep them close
- Set phone to lock after short duration (1 min.)
- Is there setting to erase data after **xx** unsuccessful login attempts or wipe data if lost?
- Update OS, apps, and programs regularly
- Use a "find my phone" app
- Download only from trusted app stores
- Don't click links in text, email, or social network

More Ways to Protect Your Smartphone

- Use ***strong*** screen lock (at least 8 characters)
- Attach a note
- Backup photos and videos
- Record your phone's unique ID number

If Phone is Lost or Missing (Gone)

- Seek and destroy
- Change important passwords
- Call your banks and other institutions
- Report loss to police
- May not be able to recover it…

Note: If your phone is recovered, wipe it anyway.

(Consumer Reports 2014)

Android Issues

- Cisco reported 99% of all malware in 2013 targeted Android devices
- Kapersky Lab gave 98% in December 2013.
- Are they over-stating the statistics because they provide security??
- Lookout reported 75% increase in Android mobile Malware encounter rates in 2014 over 2013.
- Both HP and Forsythe reported Android as biggest target in 2015

Protecting Your Devices (Android)

- Be cautious when installing apps (uncheck unknown sources)
- Watch out for phishing/SMS
- Lock Screen Security
- Consider anti-virus anti-malware, remote wipe security app software (ex: Avast, McAfee)
- Consider a parental control app
- Change the screen lock method
- Add a message to the homescreen
- Create multiple user accounts
- Activate equivalent Find My Phone

Android Security Settings

- Enable Lock Screen: Settings → Security → enable face unlock, pattern, PIN, and password
- Disable USB Debugging: Settings → USB debugging
- Enable Full Disk Encryption: Settings → Security
- Maintain Device Up-To-Date
- Stick to official app stores
- Consider an application locking app

(SecurityWatch)

Top 5 Android Security Apps

- 360 Mobile Security (Free; Google Play, Amazon)
- Avast! Mobile Security (Free; Google Play)
- ESET Mobile Security& Antivirus (Free; Google Play, Amazon)
- Avira Antivirus Security (Free; Google Play)
- AVL (Google Play)
- Other Contenders:
  - McAfee Antivirus & Security
  - TrustGo Antivirus & Mobile Security
  - Trend Micro Mobile Security & Antivirus

(the guardian.com)

Protecting Your Devices (Windows)

- RT Security Features:
  - Same "Secure Boot Technology" as full editions of Windows 8
  - Trusted Boot—runs anti-malware prior to loading the OS
  - Trusted Platform Module (TPM) Chips—allows virtual smart cards
  - Supports device encryption—can use picture passwords
  - Apps primarily from Microsoft Store = more secure
- Downside—trusting Microsoft with personal data and keys

Protecting Your Devices (Windows)

- Windows 8 Pro Security:
  - Everything in RT plus more!
  - BitLocker and BitLocker to Go—encrypt whole volumes
  - Encrypting File System (EFS)—encrypt files or folders
  - Group Policy—can be configured to enforce security policies
  - Domain Join—allows administrators to control tablets through the centralized management model which controls who accesses which resources

Protecting your Devices (Windows)

- Install antivirus software. MS Windows Defender is free and installed automatically with Windows 8.
- Ensure Defender is enabled and Windows Firewall is enabled.
- LIVE account allows for two-stage authentication and full disk encryption.
- New or upper end Surface Pro has full version of Windows 8.
- Install additional 3rd party security software
- User Account Control, File History, Windows Update, Windows Firewall, Action Center (check status of firewall, antimalware protection date, automatic update installs)—Applies to Windows 8.1, RT 8.1
- Create separate user accounts for different users
- Create a user account for everyday; only use admin credentials/account when needed
- Encryption

Protecting your Devices (iOS)

- App Store apps have been approved
- Should you jailbreak?
- Update latest iOS and security patches
  - Settings ➡ General ➡ Software Update
- Set a strong passcode; set max number of attempts before device wipes itself
- Make functions unavailable
  - Settings ➡ General ➡ Restrictions ➡ Enable Restrictions

Protecting your Devices (iOS)

- Use "Find My iPhone" app to find lock or wipe a lost device or sound an alarm. Location services must be on to find a device.
- Carefully manage location services.
- Modify Safari security settings such as autofill, fraud warning, and blocking pop-ups
- If a device is lost or stolen, change passwords on any accounts accessed by that device.
- Consider using a password management app

Reminders: To Do

- Backups
- Passcodes
- Encryption
- Find my phone/device
- Check Reputation before Downloading
- Important for us AND for our students alike!