Clean Up Your Act – Cyber Hygiene Best Practices

Photo Credit - SecurEnvoy

Jeremiah Still, PhD
Department of Psychology
Old Dominion University

Good Cyber Hygiene: Offers Protection

According to FBI's Internet Crime Complaints Center (2015):

- 288,012 complaints of cybercrimes
- 40% resulted in monetary losses
  - Average reported loss being $8,421
  - Males aged 50-59 highest victim count at 31,473
  - Females aged 40-49 highest victim count at 29,559
  - 1,648 victims reporting losses over $100,000

Social engineering and phishing attacks increased by 8% between 2015 and 2016 (2nd Annual Cost of Cyber Crime Study by Ponemon Institute).

Much of our valuable, and sensitive, data (e.g., health, intellectual property, banking) are accessible digitally

- Users love digital convenience, but are not aware of security requirements
- Users don’t perceive varying degrees of risk due to their behavior

Cyber hygiene is the best practices for maintaining performance of computing systems and the security of our data.

Successful Cyber Hygiene

- Physical Security Example,

The user:
  * Understands the value?
  * Knows how to implement it?
  * Remembers how to use?
  * Understands the limitations?

(Still, 2016; Cybersecurity Needs You!)

Issues associated with Passwords

Passwords really aren’t as strong as we think (justified by bit strength)

- Passcodes are not evenly distributed
- Cognitive short-cuts form clusters

Popular Clusters:

password, iloveyou, 123456, qwerty, abc123, hello, dragon, monkey, ninja, 1234, 1111, 0000, 1212, 7777, 1004, 2000, 4444, Password123

Issues associated with Passwords

According to Cain, Edwards, & Still (2018)-- 268 mTurk survey respondents:

- 85% used personal information
- 46% used dictionary words
- 50% used the same password for multiple accounts
- 59% do not change their passwords
- 95% share their passwords with others

They require too much cognitive effort!

- Recall retrieval processes
- Always changing (requires working memory resources)
- Generate novel content (often under time pressure)
- Not meaningful (difficult to integrate into long-term memory)

Cain, Edwards, & Still (2018)

#1: Secure your Email Account

Your email is the **master key** to most of your accounts

- Create strong passwords
- Consider using a password manger (like: 1Password)

- 2-Step Verification (e.g., gmail)
  - Use Google Authenticator {best option}
  - Text message (SMS)

Successful Cyber Attack

Depend on:

Deception (con a human)

OR/AND

Vulnerability (exploit technology weakness)

Social Engineering Attack

Misunderstanding following massive hack of 2 million passwords:

"why the hell would anyone want on my facebook for anyway? other personal stuff email, or bank account I understand. what are they gonna do with facebook, put up a post for you and look at your pictures? " (with *70 thumbs up*!) –MSN Money Blog

#2: Maintain Online Privacy

Deception (a human attack)

Do not

- Use real name on social media
- Provide phone number
- Provide birthdate
- Provide email address
- Ignore your privacy settings

Warning Signs

- Weird Requests
- Stresses their authority
- Pressures you
- Name dropping
- Compliments you
- Threatens negative consequences

Mitnick & Simon (Art of Deception)

#3: Update your Applications and Software

Vulnerability (technology attack)

Android App:
Open App Store > Settings > Auto-update

Windows Software:
Task bar > All Programs > Windows Update > Check for Updates

#4: Setup a Basic Defense @ Home

- Antivirus (e.g.,: AVG AntiVirus, Bitdefender)
- Correctly configured firewall
  - Update firmware
  - Change default passwords
  - Check Log File & Filter MAC Addresses
- Secure Wifi
  - Require Password
  - Change Network’s SSID name
  - Enable Network Encryption (WEP; WPA; WPA2)

#4: Setup a Basic Defense: Mobile Devices

- Use screen lock
- Use VPN while on Wifi hotspots
- Forget Wifi SSID you rarely use
- Disable Automatic Connect to Wifi
  - iOS: Settings > Wi-Fi
  - Android: Settings > More > Mobile Networks

- Beware of: Bluetooth Connectivity, No Voice Encryption, App Permissions, and Location Sharing

#5: Don’t Use an Administrator Account

If using a standard user account you will be rarely prompted for an admin password.

It is your last line of defense against an attack. The account reduces the amount of harm a virus can cause, which improves the odds of a full recovery.

Prompted for admin password, if

- Installing and removing software
- Changing important operating system settings
- Change or delete files in protected folders

#6: Disable Remote Desktop Protocol (RDP)

Windows Remote Desktop allows your computer to be fully accessible remotely. It is a very useful feature for tech support workers. However, it is also helpful for hackers.

If not using remote technical support disable the feature.

Start > Control Panel > System & Security > Remote Settings > **Don’t Allow Connections to This Computer**

Windows 10: type “remote settings”

#7: Back-up Files

A compromised computer often losses access to information stored on its hard drive.

- Ransomware – often blocks access to data until payment is received
- Virus – destroys and corrupts data, while spreading to other devices

Back-up your important data to the cloud or an external hard drive *regularly*

  - Set a reminder to back-up
  - Review your back-up files for completeness

#8: Encrypt sensitive files

Making it difficult for hackers to access your sensitive information

Process:

1. Find your valuable files that require privacy
2. Attempt to place all your sensitive files a few folders
3. Install an encryption tool (like: AxCrypt)
4. Encrypt your files and do not forget your passphrase

#9: Secure Your Internet Browser

- Extensions and Add-ons are considered dangerous
  - Use only a few and delete unused extensions, if they must be used
  - *Do not use them!* IE: Internet Options > Advanced tab > uncheck “enable third-party browser extensions”

- Set your preferred browser to auto update
- IE: Internet Options > Set “Trusted sites” & “Restricted sites” to High zone
  - Disable
    - JavaScipt
    - Flash
    - ActiveX
- Delete Cookies

#10: Have a Secure Computer for Accessing Sensitive Information

It is difficult to determine whether your everyday computing devices are secure. And, maintaining full cybersecurity situational awareness is impossible.

Have a secure computer ONLY for sensitive information access:

- Banking
- Health records
- Passwords
- Tax Information

Cyber Hygiene Best Practices

1: Secure your Email Account

2: Maintain Online Privacy

3: Update your Applications and Software

4: Setup a Basic Defense

5: Don’t Use an Administrator Account

6: Disable Remote Desktop Protocol

7: Back-up Files

8: Encrypt Sensitive Files

9: Secure Your Internet Browser

10: Have a Secure Computer for Accessing Sensitive Information