FORT PITT® CAPITAL GROUP

JULY 21, 2015

YOUR FUTURE IS OUR FOCUS

What does an identity thief want?

- Social Security Number
- Birthdate
- Mother's Maiden Name
- Passwords
- Driver's License Number
- PIN Numbers
- Credit Card Numbers
- Bank Account Numbers

How do you secure that information?

- Avoid sending personal information in e-mail or instant messaging
- Limit personal information you post on social media
- Avoid opening files, programs, or links from unknown senders
- Dedicate one credit card solely for online purchases
- Keep your device and browsers up-to-date
- Download firewalls, anti-virus, and anti-spyware
- Avoid storing personal information on your device
- Have strong passwords and enable two-factor

Identity Theft and Online Security

We live in a password-driven world that is pushing people towards online efficiency. With the increase in user interaction online, an increase in identity theft and security risks transpires. Identity Theft is the fastest growing crime in America. The Federal Bureau of Investigation has stated "a stolen identity is a powerful cloak of anonymity for criminals and terrorists… and a danger to national security and private citizens alike."

Online Security has grown substantially, as well, in the last ten years, becoming a major concern for individuals and institutions. On average, there are 42.8 million attacks around the world resulting in 117,339 a day. A real time map of cyber attacks can be found at http://map.norsecorp.com.

What do I do if I've become a Victim?

You are not alone. On average, there are 12.1 million identity fraud victims in the United States per year.

- Close compromised accounts
- Change your passwords
- Contact all your financial institutions immediately
- Contact a credit reporting bureau to flag your information with a fraud alert
  - Experian
  - Equifax
  - TransUnion
- File a police report
- Document everything in writing
- Keep names and dates of everyone you speak to

TRUST INSIGHT VALUE

Two-Factor Authentication

Passwords have become increasingly insecure when put up against today's top-notch hackers. Two-Factor Authentication thankfully has created a new layer of security between the hacker and your account. Two-Factor now takes advantage of three types of information - knowledge (password), physical (cell phone), and biometric (fingerprint). Essentially, it is an additional step when logging into an online account that requires something you know along with something you have. A previous blog post from Todd Douds, Protecting Yourself from Cyber Fraud, added insight to Two-Factor authentication, including a list of sites that are using Two-Factor. Companies on this list include Google, DropBox, Facebook, Amazon, Microsoft, and Apple.

Smartphone Security

Nearly two-thirds of Americans own a smartphone, and for many, these devices have indirect access to personal information. Even with antivirus protection installed on your phone, your device is susceptible to hackers searching for your personal information. Hackers can attack your phone on public Wi-Fi networks, over a Bluetooth connection, and even through the applications installed on the device. If you lose the device, it will take roughly two days for the average hacker to crack the passcode, allowing them unlimited access to your contacts, notes, GPS locations, e-mail, and any other information you store on your device.

How do you fix this security risk? Individuals should treat their mobile device like they treat their computer.

- Always have a password on the device, and utilize more complex passwords when possible.
- Keep the device up-to-date on software updates
- Only download apps from approved sources
- Check application permissions
- Turn off automatic Wi-Fi connection and Bluetooth

Business Week's article "The Problem with Passwords" discovered that a 6 character password containing only letters can be cracked in just 10 minutes while a 9 character password complete with lowercase and uppercase letters, numbers, and symbols will take 44,530 years.

How to Create a Strong Password

- Make it memorable
- Build a password with at least 8-12 characters. The longer, the better
- Utilize characters from all four categories
  - Uppercase (A, B, C)
  - Lowercase (a, b, c)
  - Number (1, 2, 3)
  - Symbol ($, &, %)
- Use different passwords for each account and try not to repeat them
- Avoid using public information
  - Birthday
  - College
  - Spouse
- Utilize the space bar by creating sentences as passwords
- Change your password frequently (every couple months)
- Store passwords securely by utilizing encrypted password managers

Informative Links

Identity Theft

http://www.fortpittcapital.com/protecting-yourself-from-cyber-fraud/

http://www.ted.com/talks/david_birch_identity_without_a_name

https://www.fbi.gov/about-us/investigate/cyber/identity_theft

https://www.identitytheft.gov/

http://www.ssa.gov/pubs/EN-05-10064.pdf

Online Security

http://www.ted.com/talks/bruce_schneier

http://www.ted.com/talks/chris_domas_the_1s_and_0s_behind_cyber_warfare

http://www.ehow.com/about_5410891_types-internet-security-threats.html

http://www.consumerreports.org/cro/electronics-computers/guide-to-internet-security/index.htm

Phone Security

http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx

http://www.informit.com/guides/content.aspx?g=security&seqNum=92

http://mobile-security-software-review.toptenreviews.com/

http://www.consumerreports.org/cro/magazine/2013/06/keep-your-phone-safe/index.htm

Email Phishing

http://www.fortpittcapital.com/phishing-scams-what-they-are-how-to-avoid-them/

https://s3.amazonaws.com/knowbe4.cdn/SocialEngineeringRedFlags.pdf

http://www.microsoft.com/security/online-privacy/phishing-scams.aspx

http://www.fraud.org/scams/internet-fraud/phishing

http://computer.howstuffworks.com/phishing.htm

Two-Factor Authentication

http://www.fortpittcapital.com/protecting-yourself-from-cyber-fraud/

http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two-factor-authentication-right-now

http://www.pcmag.com/article2/0,2817,2456400,00.asp

Passwords

http://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd

http://www.google.com/goodtoknow/online-safety/passwords/

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_en.pdf

Password Managers

https://en.wikipedia.org/wiki/Password_manager

http://www.techrepublic.com/blog/it-security/how-safe-are-online-password-managers/

Five Best Password Managers: http://lifehacker.com/5529133/five-best-password-managers

Ten Best Password Managers: http://www.pcmag.com/article2/0,2817,2407168,00.asp

Malware/Spyware/Virus Protection

Best Paid Versions: http://www.pcmag.com/article2/0,2817,2372364,00.asp

Best Free Versions: http://www.pcmag.com/article2/0,2817,2388652,00.asp

For MAC Users: http://www.pcmag.com/article2/0,2817,2406379,00.asp

Free Malware Scan: http://www.malwarebytes.org/3/

Free Spyware Scan: http://www.superantispyware.com/

Information Security for Businesses

http://www.sans.org/critical-security-controls/

http://www.nist.gov/cyberframework/