Digital Security

Digital crime is a growing problem not only in the United States, but worldwide. If you exercise caution and educate yourself, you can increase your chances of not becoming a victim of a scam or scheme.

What You Can Do

There are no "magic bullets" to keep you and your information safe from scammers, malware, surveillance, and cyber criminals. A combination of tools and techniques, however, can drastically increase your Internet security and privacy.

E-mail Scams

E-mail is perhaps the most popular way to steal sensitive information through the Internet. It is often sent and received unencrypted, and junk mail / spam filters will not catch everything [1]. Phishing scams [2] are becoming increasingly-sophisticated and are made to look like they are coming from an authentic source (a university, your financial institution, a personal contact). Although such e-mails may be legitimate, they may also be an attempt to scam you out of your money – never give or send cash/check without seeing and receiving the goods in question. Your personal and credit information should never be treated casually, or traded for promises of money, housing, or employment. **If a deal sounds too good to be true, it probably is.**

Tips to Protect your E-mail

- Microsoft - Phishing [3]
- E-mail Self-Defense [4]

Immediately report e-mails that look like phishing or contain suspicious links to abuse@yale.edu **[5].** [5] To determine the actual origin and to make a full investigation possible, ITS requires that you provide the full header of the message.

If an e-mail seems to be part of a bigger, non-phishing scam (housing/rental scam, asks for credit card, etc.) send a copy to safe@yale.edu **[6]**.

Passwords

Creating a Strong Password

The object when choosing a password is to make it as difficult as possible for someone (or some computer program) to guess what you've chosen, yet easy enough for you to remember without writing it down.

Secure Password Storage

No one likes to remember the multitude of passwords required to live a "digital life." However, creating diverse passwords for different programs and websites is very important. For this reason, many people write down passwords on paper post-it notes or keep a spreadsheet on their computer. A much safer way to store these passwords is to install and configure software specifically designed to safely contain your passwords, such as LastPass [7]. Most modern browsers now offer to save passwords as well, so be sure to properly secure the device that they are installed on [8] so that no one gets access to your saved passwords.

More Password Tips:

- xkcd [9], a popular Web comic, recommends a secure pass phrase scheme in this easy graphic [9].
- Such pass phrases are difficult to guess, but easy to remember. Try creating your own here [10].
- Security expert Bruce Schneier offers his advice on secure passwords [11].

Security Starter Pack

The Electronic Frontier Foundation [12] offers "playlists" to guide you through cyber security basics. These resources will help you discover how to assess your personal risk, protect your most cherished communications and information, and start thinking about incorporating privacy-enhancing tools into your daily routine.

1. An Introduction to Threat Modeling [13]
2. Communicating with Others [14]
3. Creating Strong Passwords [15]
4. What Is Encryption? [16]
5. Keeping Your Data Safe [17]
6. Protecting Yourself on Social Networks [18]
7. Choosing Your Tools [19]

Print Materials

For a more detailed, explanatory booklet, refer to Susan McGregor's excellent guide for journalists [20]. It contains basic explanations and diagrams relevant for every Internet user.

Software Options

To better choose software that will respect your privacy and security, refer to the resources below.

- Security In-A-Box [21]
- Better Web Browsing [22]
- PRISM Break [23]
- E-mail Self-Defense [4]

Software at Yale

Yale ITS is the authority on specific software in use at Yale, and what you can do to protect sensitive data inside and outside the Yale network. Please take a look at the helpful ITS guides below.

- Connecting to the Yale VPN [24]
- Backing Up and Securing Devices [25]
- Box at Yale Cloud Storage [26]

Source URL: https://oiss.yale.edu/life-at-yale/safety-security/digital-security

Links:
[1] http://www.zdnet.com/article/phishing-experiment-sneaks-through-all-anti-spam-filters/
[2] http://www.phishing.org/

[3] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing
[4] https://emailselfdefense.fsf.org/en/
[5] mailto:abuse@yale.edu
[6] mailto:safe@yale.edu
[7] https://www.lastpass.com
[8] https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device
[9] https://xkcd.com/936/
[10] http://preshing.com/20110811/xkcd-password-generator/
[11] https://lifehacker.com/228887/bruce-schneier-on-how-to-choose-secure-passwords
[12] https://ssd.eff.org/
[13] https://ssd.eff.org/en/playlist/want-security-starter-pack#introduction-threat-modeling
[14] https://ssd.eff.org/en/playlist/want-security-starter-pack#communicating-others
[15] https://ssd.eff.org/en/playlist/want-security-starter-pack#creating-strong-passwords
[16] https://ssd.eff.org/en/playlist/want-security-starter-pack#what-encryption
[17] https://ssd.eff.org/en/playlist/want-security-starter-pack#keeping-your-data-safe
[18] https://ssd.eff.org/en/playlist/want-security-starter-pack#protecting-yourself-social-networks
[19] https://ssd.eff.org/en/playlist/want-security-starter-pack#choosing-your-tools
[20] https://susanemcg.gitbooks.io/digital-security-for-journalists/
[21] https://securityinabox.org/
[22] https://riseup.net/en/security/network-security/better-web-browsing
[23] https://prism-break.org/en/
[24] https://its.yale.edu/how-to/article-setting-up-vpn-your-mobile-device
[25] https://your.yale.edu/technology/data-security/other-data-security-resources
[26] https://yale.service-now.com/it?id=service_offering&sys_id=ff584dcd6fbb31007ee2abcf9f3ee4ee