Tech Resources for Privacy, part II

General Cybersecurity Guidelines

These are general guidelines for computer safety, but perpetrators can use these vulnerabilities to continue to abuse their victims.

- Don't click on a link in an email or text unless it is from a source you trust AND you are expecting it. It is better to search for the website on Google or type in the link yourself in a web browser.
- Don't open any email or message attachments unless it is from a source you trust AND you are expecting the file.
- Make sure you stay current with software updates for all your devices and apps.
- Try to use strong passwords that are unique to each account/site you use.
- Use multi-factor authentication (MFA) if you can.
- Never give out your password over the phone.
- Posts on social media are never truly private, no matter your settings: once it's online, it's no longer under your control. Be protective of your personal information and remember that phone numbers, addresses, handles, and personal details (like birth date, schools you attended, employers, and photos with landmarks) may make it easier for someone to reach you.
- Set boundaries and limits, and ask people not to post personal information, photos, or check-ins you aren't comfortable with. Check your social media settings to make sure your privacy settings are strict, and disable the ability for other people to tag you in their photos or posts. Similarly, don't post information about people without their consent – you could jeopardize their safety or the safety of others.

Passwords

The average Internet user has dozens of accounts across dozens of websites, and while password management can be difficult, it is very important to be careful with passwords. A perpetrator can cause a lot of damage if he can figure out how to log in to one of your accounts.

- The length of a password is more important than its complexity. Consider using the name of a favorite song; don't use your kids' names or birthdates or something he could guess. Try to use a password that is at least 10 characters long.
- Try to use passwords that are unique to each site. Don't reuse the password, for instance, you use for banking to be your email password also.
- Try not to write down your passwords, especially in a place he could find. Assume he is going through your belongings when you are not there and that he is snooping around. He may get suspicious and that will increase the intensity of his searches.
- However, if you can't remember your passwords and need to record them, it is better to physically write them down than to store them electronically on your phone. Or worse, keep forgetting your passwords and resetting them.

Tech Resources for Privacy, part II

Cell Phone Safety

We rely on our cell phones to help run our lives, but they can become a weapon in the hands of perpetrators if we don't treat them carefully.

- Put a passcode on your phone to make harder for someone to get into it.
- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.
- Do not respond to any questions, especially those that can be answered with "Yes" or "No." The caller can record your voice, and then play it back later for nefarious purposes.
- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. There are many services and apps that can spoof phone numbers and names.
- Use caution if you are being pressured for information immediately.
- If you have a voice mail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.

Device Safety

Computers, laptops, and tablets need strong security also.

- Put a password on your computer or laptop.
- Avoid clicking on links or opening attachments sent to you by someone you don't know or someone you think might want to monitor your computer activity.
- Run anti-virus and anti-spyware software on your computer, and make sure that it automatically updates so you have the latest protection.
- In some cases, you might have to share documents with the person you are concerned is trying to monitor you. Consider using online sharing platforms, such as Google Docs, Dropbox, or Flickr, to exchange information rather than having it come directly into your email.
- Be cautious when using a computer that is not yours. Log out of accounts, erase your activity from the web browser, and don't save personal items onto that computer. If you must save something to the computer, delete it, including from the trash.