Information Security Overview

Every day, it seems there is another news story about the latest data breach, ransomware attack, or other security related threat. ***Please*** take the time to read this page in full, and implement the advice contained here. Remember, the first defense against any malware attack or identity theft is **you**, the user.

Identity and Data Security

Account Security

Q: How do I keep my accounts secure?

A: We recommend that you use a different password for every account you have. Each password should be unique and complex. A complex password contains a minimum of 8 characters. The key to a secure password is the longer the better. You can also include at least one lowercase letter, one uppercase letter, a number, and symbol. See Secure Password Management to learn where you can store all your passwords securely and in one place.

Email-Related Threats

Phishing

When reading your emails, always stay vigilant. If you receive an email—and something seems fishy about it—always listen to your gut. An email may look completely legit, but a corporation will never ask for you to email them things like your password or credit card information in plain text. Look at the URLs of the links in the email. Check the sender's email address. Never open a suspicious attachment. If something seems off, it probably is. The scam artists are getting much more sophisticated at seeming legitimate, but if you use a little bit of common sense, you should be able to catch when things don't feel right, and act accordingly. More information about how to detect phishing attempts and how to report phishing emails can be found in Google's Gmail Help Center.

Email attachments

Never open a suspicious attachment! And generally, do not open attachments that you were not expecting, or aren't from a trusted source. Gmail, and most webmail services have good malware scanning built in these days, but if the file is over 25MB, the scan won't run. Be careful, and stay vigilant. Again, practice common sense.

Phone-Related Threats

Scam Calls / Robocalls

If you receive a phone call that seems suspicious, whether it's a computer-generated voice on the other end or a person fishing for personal information: Don't follow any directions given by the caller. Just ***hang up the phone***. Following any prompts given by the caller may make them more likely to call again. ***Never give out any personal information*** to an unknown caller. Take down any information you remember and report the call to the FTC.

These calls often show up as being from a local phone number, spoofing of numbers is rampant among scam callers, to hide the call's origin and make the calls difficult to block.

Identity Theft/Hacked Account

Q: Help! My account has been compromised, what can I do?

A: The first and foremost thing you should do if you still have access to your account is to change all your passwords and security questions, along with anything associated with your account. Let your contacts know that your account has been compromised and to not open any suspicious

emails from you. After updating your passwords and security questions, check your email settings and make sure nothing has been changed. It is not uncommon for hackers to modify your recovery email address and automatically forward your emails to them. Scan your computer for malware and viruses (See our Anti-Malware Software section). For more information on securing your account:

- Secure an account that has suspicious activity (Google)
- Recover a hacked or hijacked account (Google)

Password Managers

Q: There are too many passwords to remember! What can I do?

A: LastPass is a password manager for all of your devices. LastPass is great for storing passwords for websites, web services, or just about anything else. It's more convenient and secure than your web browser's password manager, in that you can connect on all your devices. There is a LastPast Website and web add-on, a desktop application, and a mobile phone app. This means you only need to remember one password to have access to your passwords on all your devices.

You can download LastPass from here: https://lastpass.com/misc_download2.php

Q: How do I get started with LastPass?

A: Visit the LastPass User Support Page to learn how to make your profile secure and customize to your preferences.

There are some configuration settings you will want to get familiar with:

- Master Password - the one password you will need to remember to gain access into your LastPass account.
- Account Settings - add a recovery email or phone number, manage preferences, etc.
- Auto Logout - ensure LastPass logouts of your account when you are away from your device.

For a more detailed write-up on password management software, go here.

Anti-Malware Software

Q: How do I keep my computer secure?

A: We recommend downloading an antivirus and anti-malware software. To keep your computer secure, make sure that you keep your antivirus/anti-malware software up to date.

Windows 7 and **older**

- Microsoft Security Essentials - Unobtrusive, effective, and free.
- Malwarebytes Anti-Malware - Has solid malware definitions. Run when you suspect that Microsoft Security Essentials missed something, although it doesn't hurt to run it more often.

Windows 8 and **newer**

- **Windows Defender -** The successor to Microsoft Security Essentials, included with the operating system. You don't have to install any extra software.
- Malwarebytes Anti-Malware - Has solid malware definitions. Run when you suspect that Windows Defender missed something, although it doesn't hurt to run it more often.

Mac OS X

- ClamXAV - An antivirus software for Apple Macintosh provides full disk virus scans, scheduled scans and updates for times that suit you, automatic scanning of new downloads, quarantining infected files, and much more. Consider installing the free 30-day trial initially.
- Malwarebytes Anti-Malware - Has solid malware definitions in addition to an effective heuristics engine that will check your computer for software with suspicious behavior.

Network Security

Adblock

Q: What is an adblocker and which one should I use?

A: An adblocker is a web browser extension designed to prevent ads from appearing on a web page. Adblockers are useful on websites with questionable content where clicking on an ad may result in your computer downloading malware. We recommend uBlock Origin, which is available for Chrome, Firefox, and Edge.

Clear Web Browser Cache

Clearing your web browser's cache can help fix problems related to accessing web sites. If you are having problems accessing or otherwise using a website that you believe should be accessible and functioning normally, try clearing your browser's cache to fix the problem.

Q: How do I clear my browser cache?

Mozilla Firefox:

1. Click the menu icon (the three stacked horizontal lines near the top right of your browser window).
2. Click **History**, then choose the **Clear Recent History...** option.
3. Select the **Time Range** to clear (drop-down menu).
   - Select **Everything** to clear all cache.
4. Click **Details** to choose what history elements to clear.
   - e.g. Cache, Cookies, and Active Logins
   WARNING!: DO NOT check the Browsing & Download History or the Form & Search History boxes.
5. Click the **Clear Now** button.
6. Exit and re-launch the browser.

Google Chrome:

1. Click the menu icon (the three stacked horizontal lines near the top right of your browser window).
2. Hover your mouse cursor over the **History** menu option, then click **History** at the top of the expanded menu.
3. Click **Clear browsing data...**

4. Set the **Obliterate the following items** from drop-down menu to **the beginning of time**.
5. Check the **Cookies and other site and plugin data** and **Cached images and files** boxes ONLY. (Un-check all other check boxes)
6. Click the Clear browsing data button.
7. Exit and re-launch the browser.

Safari:

1. Open Safari.
2. Click on **Safari** in the upper toolbar and select **Clear History...**
3. Select **all history** from the drop-down list.
4. Click the **Clear History** button.
5. Quit and re-launch the browser.

Update Web Browser

Q: Why should I update my web browser?

A: It is important to always run the most updated version of your web browser. Using an outdated web browser can compromise the security of your computer and any networks to which it is connected. Web browser developers are constantly searching for security vulnerabilities and when they find them they fix them and update the software. Therefore, if you are running a later version of a browser you are leaving yourself vulnerable to malicious websites.

Do not use browsers that no longer have updates or are being retired (e.g. Safari for PCs, Internet Explorer).

Q: How do I update my web browser?

A: It is highly recommended to set up your browser to automatically update. For update instructions and how to set up automatic update follow the link for instructions for your specific browser:

- Google Chrome: this browser's default is to automatically update
- Firefox: this browser's default is to automatically update
- Safari: this browser updates with macOS updates
- Edge: this browser's default is to automatically update

NOTE: If the instructions outlined here do not match the menus and options in the web browser you are using, please check to be sure that you are using the most recent version of the web browser. Using an outdated web browser can compromise the security of your computer and any networks to which it is connected.

Revision #22
Created 13 February 2019 18:34:24
Updated 12 November 2021 23:59:40