TASC

Commonwealth of Massachusetts Group Insurance Commission

TASC ONLINE ACCOUNT SECURITY

TASC advises all participants to follow these instructions. Remember that security is an ongoing process. Regularly reviewing and updating your security measures is essential to staying ahead of potential threats and maintaining the safety of your online accounts.

It takes just a few minutes to put these identity theft protection safety practices into place. And with an investment of a small amount of time you can have the peace of mind that you and TASC are making every effort to protect your information. *See also:* **Protecting Your TASC Benefits (MA-6781)**

The content presented on this page and the next is excerpted from an article by Matt Burgess that originally appeared online in WIRED.

There's no foolproof way to identify every type of phishing effort or scam—scammers are constantly upping their game—but being aware of the threat can help reduce its effectiveness. Be cautious, think before you click, and download files only from people and sources you know and trust. Below are some areas where you might consider taking action on to protect your information and online accounts.

Update Everything

Update every piece of technology you use; anything from the Facebook app on your phone to the operating system that controls your smart lightbulb is open to attack. Thankfully, companies are always finding new bugs and fixing them. That's why it's crucial you download and update the latest versions of the apps and software you're using.

Start with your phone. Navigate to your device settings and find out what operating system you're using, and update it if you're not on the latest version. For apps and games, Apple's current version and above downloads updates automatically, although these settings can be customized. On Android, auto-updates can also be turned on by visiting the settings page in the Google Play Store.

Encrypt Everything

Protecting your communications has never been easier. Over the last half-decade, companies handling our personal data—including the messages we send and the files we upload to the cloud—have realized that encryption can help them as well as their customers. Using encrypted services means that what you're sending is better protected against surveillance and won't be accessible if your device gets lost or stolen.

There are two main end-to-end encrypted messaging services, Signal and WhatsApp. Messages (including photos and videos) plus voice calls and video calls are encrypted by default within both apps. They both also let you use disappearing messages, which remove what you've sent after a set period of time. The practice can help keep your chats private, even from those that have access to your devices. Our advice is to use Signal where possible, as it collects less metadata than WhatsApp and isn't owned by Facebook. But if you can't get your friends to move to Signal, WhatsApp offers a lot more protection than apps that don't use end-to-end encryption by default.

For your emails, you could choose to obtain an encrypted provider. An encrypted provider can protect your messages, and many times this affords you use of burner email accounts for mailing lists and purchases where you don't want to hand over your personal data.

Beyond your emails, encrypting the files on your devices can help reduce the chances of your data being compromised if you're hacked or lose your devices. Both iPhone and iOS encrypt your hard drive by default. Just make sure you use a strong password or PIN for your devices. A little more effort is needed to encrypt the hard drive on your laptop or computer. Turn on Apple's FileVault to encrypt your startup disk, and on Windows you can turn encryption on through the Settings menus or use another type of encryption.

Wipe Your Digital Footprint

The old online accounts you no longer use and the login details that belong to them can be weaponized against you if you don't do anything about them. Hackers frequently use details from previous data breaches to access the accounts people currently use.

Reducing the amount of information that's available about your online life can help cut your risk of being hacked. A very simple step is to regularly delete your Google search history, but you can also use privacy-first Google alternatives.

WIRED | 27 August 2021

Burgess, M. (2021, August 27). 6 things you need to do to stop yourself getting hacked in 2021. *Wired.* https://www.wired.co.uk/article/how-to-avoid-hacking

Here are **16 steps** that you can take today to help secure your online accounts and information.

01. **Use Strong Passwords.** Using strong and unique passwords for each account can significantly reduce the risk of unauthorized access. Make sure your passwords include a mix of letters, numbers, and special characters. Avoid using easily guessable information like birthdays or names.

02. **Update Passwords.** Change passwords regularly, ideally every few months.

03. **Use a Password Manager.** Consider using a reputable password manager to generate, store, and autofill complex passwords for your accounts.

04. **Enable Multifactor Authentication (MFA).** Whenever possible, enable MFA for your accounts. This adds an extra layer of security by requiring a second form of verification in addition to your password.

05. **Update Recovery Information.** Ensure that your recovery email address and phone number are up-to-date. These are important for account recovery.

06. **Use Encrypted Connections.** Ensure that you're using secure, encrypted connections (https://) when accessing websites and services.

07. **Secure Networks.** Whenever possible, use secure and trusted networks for sensitive transactions to prevent potential hacking on public Wi-Fi.

08. **Avoid Phishing.** Be cautious of emails or messages that ask for your personal information. Always verify the sender's identity before sharing any sensitive data.

09. **Regular Checks.** Regularly reviewing your account activity for any unusual transactions or login attempts is a good practice. **Make sure you're set up to receive notifications or alerts, especially on your financial accounts.** If you spot anything suspicious, take action immediately.

10. **Software Updates.** Keeping your devices and software up to date ensures you have the latest security patches to protect against potential vulnerabilities.

11. **Check App Permissions.** Review the permissions you've granted to third-party apps. Revoke access for apps you no longer use or trust.

12. **Privacy Settings.** Check the privacy settings of your accounts and adjust them according to your comfort level. Limiting the information you share publicly can help reduce your exposure.

13. **Educate Yourself.** Learn about common hacking techniques and scams to better recognize potential threats. Keep yourself informed about the latest security threats and best practices through reputable sources.

14. **Support.** If you're ever uncertain or notice something unusual, don't hesitate to reach out to the platform's support team for assistance.

15. **Review and Remove Unused Accounts.** Review your online accounts periodically. If you no longer use an account, consider deleting it. This will reduce the amount of spam you get and reduce the number of ways hackers can target you.

16. **Regular Maintenance.** Just like with other aspects of life, online security requires ongoing maintenance. Set aside time periodically to review and update your security measures. Regularly back up important data to an external source to prevent data loss in case of a security breach.