HELP PROTECT YOURSELF

Your Digital Security Checklist

Run through this list of quick, effective actions to help you improve the security of your devices and data all year long.

Managing the security of personal data can feel like you're moonlighting as your own IT manager. But it doesn't have to be be a full-time job. A handful of simple actions can go a long way toward helping prevent the worst-case scenarios, such as identity theft or financial fraud. Making a few resolutions about ongoing behavior can add another layer of security.

In this spirit, we've compiled the following checklist to provide more security with less effort.

CHECK YOUR FINANCES

- ☐ **Set up alerts.** Stay in touch with your account and card activity by enrolling in Huntington's alerts[1]. Notifications like low balance, withdrawals, international charges, and 'card not present' can help alert you to activity that is not yours. Confirm It fraud alerts send an email or text when a charge on your credit card looks suspicious. If you spot something fishy, Huntington lets you lock and unlock cards online or from your smartphone.

- ☐ **Get your annual free credit reports.** By law, Experian, Equifax and TransUnion must provide you with one free report a year, and you can space out your requests to get one every four months. Make sure your personal data is up to date, then look for inaccuracies in entries about loans and credit cards. Check out our Credit Report Educator for tips on reading your report.

- ☐ **Consider freezing your credit.** If you freeze your credit, no one but you can pull your credit report, which makes it more difficult for identity thieves to open accounts in your name. Freezing your credit is free, but you have to contact each of the credit agencies individually.

CLEAN UP YOUR PASSWORDS:

- ☐ **Change any repeated passwords.** A data breach can often leave your passwords exposed—which is especially troublesome if you use the same or similar passwords for all of your accounts. Unique passwords are your best defense. Start by setting them up on your major accounts—bank, credit card, email—then work your way through any other repeats a few at a time. Learn how to make hard-to-guess buteasy-to-remember passwords here.

- ☐ **Consider using a password manager.** These apps, which range from free to $60/year, generate strong, unique passwords and fill them in when you log into a site from a computer or smartphone. Password managers stash your heavily encrypted password list either in the cloud or locally, behind a master password you create. Learn more about password managers here.

- ☐ **Sign up for two-factor authentication (2FA).** 2FA is simpler than it sounds: It just means you have to enter something in addition to your password when you log in, usually a code you get from a text message or an app on your phone. It only adds a few seconds to your log in, but renders a stolen password nearly useless.

[1] *Carrier's message and data rates may apply.*

UPDATE YOUR DEVICES AND ACCOUNTS

- ☐ **Update the software on all your devices,** including your computer, phone, router, voice assistant and security system. Updates often contain security fixes such as patches for recently discovered vulnerabilities or malware. The easy-to-ignore part of this is the home router, but remember it's the gateway to your whole homesystem. You may have to dig in the settings to find the option to update. Any time you see a setting for automatic updates, turn it on.

- ☐ **Make sure your computer backups are up to date.** Should malware take down your computer or phone, you need a backup that's current and easy to access, whether on a separate hard drive or a cloud-based service. Cloud services start at about $50/year for unlimited storage[2] and work in the background. If you do have a backup system, log in to make sure it's still working and that you know how to restore files.

- ☐ **Check the privacy settings on social media accounts.** Social media sites periodically update their privacy and information sharing practices. Log in and make sure the privacy settings match what you want them to be. Other things to check while you're there: Advertiser settings (whether or not the service can share your information with third parties) and location-tracking settings.

SECURE YOUR HOME NETWORK

- ☐ **Change the default password on your router, then do it for the rest of your device.** With just a quick internet search, hackers can find the preset factory login for just about any gadget. With that they have free reign to hijack and/or install malware on your device. Login credentials are usually in these settings. Don't forget to use unique passwords.

- ☐ **Set up a guest WiFi newtwork.** Your home network is only as safe as the least protected machine connected to it—and that could belong to a guest. With most modern routers, adding a guest network is as easy as flipping a switch in the settings. Make sure everyone in the family knows about the guest network and directs visitors to use it.

- ☐ **Turn on the firewall in your router and laptop.** Your router is the first line of defense for every device connected to it; the firewall prevents unrecognized or dangerous incoming connections. Activate your laptop's firewall for added protection when you're on other networks. It's a simple switch in the settings and shouldn't affect your internet speed.

Contact Huntington

If you think you may be a victim of fraud related to your Huntington credit or debit card, or your card has been lost or stolen, please let us know right away at **(800) 480-2265**.

If you receive a suspicious email claiming to be from Huntington, please let us know at **ReportFraud@huntington.com**.

Visit **huntington.com/Security** for more tips on protecting yourself and to learn more about how we help protect your privacy and keep your information secure.

[2] *Kissell, Joe. Wirecutter. The Best Online Cloud Backup Service. October 23, 2018*