Huntington Welcome.®

Your personal information is like money. Value and protect it.

These days, we spend much of our personal and professional lives online, so it's more important than ever to protect your personal information from people who want to steal it and businesses that want to use it. Your personal data, such as bank account information, social security number, and email address, are worth a lot of money.

DID YOU KNOW?

Only 12% of surveyed U.S. adults are "very confident" in the ability of the federal government to protect their data.[1]

[1] Source: Americans and Cybersecurity. Pew Research Center.

6.95M new phishing and scam pages were created in 2020.[2]

[2] Source: Top cybersecurity statistics, trends, and facts. CSO Online.

More Americans surveyed are worried about their data privacy than they are about losing their main source of income.[3]

[3] Source: TRUSTe/National Cyber Security Alliance U.S. Consumer Privacy Index 2016.

Knowledge is a powerful tool to help protect your information.

☑ Helping to protect against viruses, ransomware, and other malicious code

- Use unique, complex passwords.
- Create a naming convention to build easy-to-remember yet unique passwords for each account. For instance, the first letter of each word in a sentence: My Password Is My Dog Fluffy Twelve becomes MPIMDF12.
- Change your passwords at least three times a year as well as after notification of any account compromise or data breach. Consider using a password manager. It stores your passwords, generates strong passwords for you, and you'll only need to remember the master password for your password manager.

☑ Managing your privacy settings

- It's critical to manage the privacy settings for different online accounts and applications to ensure that you aren't giving companies or individuals access to information that you want to keep private. Manage social network privacy settings so that you can control who sees your information, posts, location, etc.

☑ Being wary of free Wi-Fi networks

- Online thieves often use unprotected Wi-Fi networks to steal passwords and other data while they are in transit. Avoid using free, public Wi-Fi, particularly in cafes, airports, etc. If you must use an unprotected Wi-Fi network, be sure that HTTPS is enabled for any sites you visit. Look for the "S" after HTTP at the beginning of the website address. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection on the go.

☑ Learning to recognize and avoid phishing attacks

- Email, phone, and text phishing attacks are popular tactics for cybercriminals. Why is that? It's often faster and easier for an attacker to trick another person rather than conducting complex, manual hacking attacks. Phishing attacks typically have telltale signs such as unfamiliar senders, strange domain names, spoofed web pages or emails, and messages with links or attachments that you didn't request.

☑ Keeping operating systems and applications updated

- Software updates, including anti-virus and anti-malware, typically contain fixes for known security vulnerabilities, so it is important to keep all operating systems and applications updated to help reduce your risk of a cyberattack. This includes mobile devices as well. Additionally, wherever possible, you should enable automatic updates.

☑ Avoiding oversharing on social media

- Cybercriminals often harvest information from social media sites to prey on victims' trust while exploiting their emotions. Be cautious about what you share on social sites. Even if you have restricted privacy settings, attackers could still see info if they have control of someone else's account.
- Consider not completing all facets of your social media profile. The people who need to know your birthdate, email, and phone number already have them.

☑ Encrypting, archiving, or deleting data you don't need

- Data encryption is not just for companies. There are many tools (some free) that encrypt your personal data, helping to keep it unreadable and safe.
- Always encrypt sensitive data before copying to removable devices such as USB storage or portable hard drives. This will help ensure that sensitive information isn't at risk if a device is lost or stolen.
- If you no longer need data, delete, or encrypt it and move it to an offline storage device, particularly old bank statements, contracts, bills, health records, and work documents.

☑ Protecting your social security number

- Be cautious when asked to provide your social security number—you will want to ensure they have a valid reason for the request and you are confident in the recipient's intentions.
- By having your SSN and information such as your date of birth or address, someone could steal your identity and open credit cards, loans, or file for unemployment in your name.

☑ Locking down your hardware

- Since so much of our personal data is stored on or can be determined from our laptops, phone, and other devices, require a password/passcode or biometrics to access your devices.

☑ Giving inaccurate answers when setting security questions

- "What is your mother's maiden name?" or "In what city were you born?" are common questions to supposedly keep an online account safe. In reality, there's nothing secure about these generic questions. Someone could easily find the answers with Internet research. You can enter any answers to these questions, even inaccuracies, as long as you can remember them later.

Contact Huntington

If you receive a suspicious email, call or text about your Huntington account, or think your personal account data has been compromised, let us know.

(800) 480-2265 | ReportFraud@huntington.com

For more information about phishing or your privacy and security, visit huntington.com/Privacy-Security