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 who want to use it. Your personal data, such as bank account information, social security number and email address are worth a lot of money.

TAKE THESE STEPS TO PROTECT YOUR INFO AS IF IT WERE CASH:

☐ 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 news of an account compromise or data breach.
- Consider using an online password manager. It stores all your passwords, generates strong ones for you, and you'll only need to remember the password for your password manager.

☐ Manage your privacy settings.

- It's critical to manage the privacy settings for different online accounts and applications. This is still the best way 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.

☐ Be 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 across networks. 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 secure connection on the go.

☐ Learn 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.

☐ Keep operating systems and software updated.

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

12%

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

500%

jump in social media-based phishing attacks from 2015 to 2016 [2]

More

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

1 Source: Americans and Cybersecurity. Pew Research Center.
2 Source: Q4 2016 & Year Review. Threat Summary. Proofpoint.
3 Source: TRUSTe/National Cyber Security Alliance U.S. Consumer Privacy Index 2016.

☐ **Avoid 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 tight privacy settings, attackers could still see info if they have control of someone else's account.
- Consider not completing your social media profile. The people who need to know your birthdate, email and phone number already have them.

☐ **Encrypt, archive or delete data you don't need.**

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

☐ **Protect your social security number.**

- Think twice about sharing your social security number (SSN) – even the last four digits – with anyone other than your financial institutions, credit bureau, a company authorized to do a background check for you or an entity that has to report to the IRS.
- By having your SSN and information such as your date of birth or address, someone could steal your identity and open credit cards, loans, etc. in your name.

☐ **Lock 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 to access your devices.
- Install an app that will locate your device if lost or stolen and will lock it or wipe it clean so a stranger can't access your information.
- Regularly back up important data in case your device is lost or stolen.

☐ **Give 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 as long as you can remember them later.

Contact Huntington

If you receive a suspicious email, call or text, or think your account data has been compromised, let us know. We'll help you determine the legitimacy of suspicious messages and account activity.

PHONE: **(800) 480-2265**

EMAIL: **ReportFraud@huntington.com**

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