PROTECT YOUR DIGITAL IDENTITY

Everything that you share and do online creates thousands of unique data points about you. This data makes up your digital identity and can include sensitive information such as passwords, bank account numbers or even your favorite cuisine noted in a dating app profile. Other data points are code that can identify your devices or geographic location. Malicious actors can gather enough of this data from multiple sources to impersonate you or to steal your identity for nefarious purposes, such as racking up massive amounts of debt in your name. Protect your digital identity the same way you safeguard your bank account PIN.

YOUR DIGITAL IDENTITY MAY INCLUDE:

DATA ATTRIBUTES

Information traditionally used to identify oneself now available online

- Username and passwords for online accounts
- Place/date of birth
- Home address
- Family members
- Social Security number
- Driver's license or passport numbers
- Eye color
- Credit card numbers
- Medical history
- Make/model of your car

ONLINE ACTIONS/ ACTIVITIES

Information voluntarily shared online or by one's online activities

- Social media profile information
- Online searches
- Online purchases and bank transactions
- Posts/photos shared on social media channels
- Group affiliations
- Apps downloaded

THIRD-PARTY DATA

Information available online due to third parties

- Degrees and diplomas
- Credit scores
- Employment history
- Criminal record

TIPS TO HELP PROTECT YOUR DATA ONLINE

Use multifactor authentication whenever available, including for your email account. This means use more than one method to verify who you are (password + one-time passcode; password + fingerprint). Your email account is often utilized for recovery of compromised accounts, so it is imperative that you protect it against cyber criminals. Other tips to protect your digital identity include:

- Avoid public Wi-Fi. Consider using a VPN to encrypt.
- Create strong passwords and a unique password for every account.
- Don't post personal information on social media or public sites.
- Don't geotag photos/videos.
- Monitor your credit report and financial accounts for unexpected activity.
- Install and update security patches and software.
- Avoid public charging stations.
- Update your operating systems, browsers and apps.
- Read Terms and Conditions before downloading apps or joining social media channels. Search for key phrases in the text like "marketing," "control," "waive" or "opt-out." Some of these phrases can lead to key insights on how the company plans to collect and use your information or can identify ways that you can update your personal privacy settings to limit what information is shared.

CON PDF 0820 0145

PNC BANK