Identity Management Tips and Advice

July 1, 2022 | National Cybersecurity Alliance

Everyone has a digital identity made up of large amounts of personal data that exists about you online.

Whether it comes from your social media profiles, search engine history or email accounts, your information is incredibly valuable to cybercriminals. If an account is compromised, your data may be stolen by cybercriminals, with the intention of stealing money, conducting phishing attacks against others, and even committing identity theft. Protect your digital identity with the following best practices:

Configure security settings

Every time you sign up for a new account, download a new app, or get a new device, immediately configure the privacy and security settings to your comfort level. Check the settings on old accounts and delete any apps or accounts you no longer use.

- **Why?** Attackers are likely to try the default login information for internet connected devices – typically admin – to try and gain access. While the default settings for most online accounts provide the website owner with the most information for a personalized experience, loose privacy settings could mean your data is being shared without your knowledge.

Think before you click

If you receive an enticing offer via email or text, don't be so quick to click on the link. Instead, go directly to the company's website to verify it is legitimate. If you're unsure who an email is from—even if the details appear accurate—or if the email looks "phishy," do not respond and do not click on any links or open any attachments found in that email as they may be infected with malware. Report phishing to your organization's IT department or your email provider.

- **Why?** Attackers often send fraudulent email and text messages, referred to as phishing, in order to trick individuals into providing information such as usernames and passwords, or to download malware.

Share with care

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others. Consider creating an alternate persona that you use for online profiles to limit how much of your own personal information you share.

- **Why?** Personal information readily available online can be used by attackers to do a variety of things, including impersonation and guessing usernames and passwords.

Use multi-factor authentication (MFA)

MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

- **Why?** At least 15 billion passwords are for sale on the Dark Web. A second method of authentication provides extra protection even if a username and password is compromised.

Download a password manager

Use password managers to generate and remember different, complex passwords for each of your accounts. 57% of workers write down passwords on sticky notes, and 62% share passwords via SMS and email, according to Keeper Security. Password managers offer secure ways to send passwords and other login credentials to family members or coworkers.

- **Why?** Duplicating passwords or using common passwords is a gift to hackers. If one account is compromised, a hacker will typically try the same username and password combination against other websites through "password spraying."

Update your software

Keep all software on internet connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware. Configure your devices to automatically update or to notify you when an update is available.

- **Why?** Software updates often fix security flaws. Outdated software can be riddled with security holes easily exploited by attackers.

If you believe your identity has been compromised, contact the Identity Theft Resource Center.

For more tips and advice, visit www.identitymanagementday.org.

*[**SOURCE**] NATIONAL CYBERSECURITY ALLIANCE: https://staysafeonline.org/online-safety-privacy-basics/identity-management-tips-and-advice/*