KnowBe4

SECURITY HINTS & TIPS

Protect Your Personal Information

For years, we've been warned not to share too much personal information with people we meet online. Now, you can shop online for almost any product, manage your finances with online banking services, and chat with friends and strangers on social media platforms. While you enjoy all the conveniences of modern technology, are you paying attention to all the ways that it can be used against you? Let's take a look at ways that you can protect your personal information.

Guard Your Login Credentials

If cybercriminals steal your login credentials, they can access your accounts and find your personal or professional information. Follow these tips to protect your accounts:

- Don't enter your login credentials unless you are certain that a website or app is secure.
- Use unique passwords for each of your accounts. A password manager can help you keep track of all your passwords, and multi-factor authentication (MFA) can add another layer of security.
- Use passwords and update the security software for all of your devices. In addition to computers and smartphones, there are several other devices that can connect to the internet. If you don't protect these devices, they can be vulnerable to hacking, too.

Be Aware of Data Tracking

When you're online, your activity can be tracked by the websites that you visit and by third parties who collect data through those websites. Data tracking allows websites to remember your preferences, but it also allows third parties to use your information in ways that don't benefit you. Follow these tips when browsing the internet:

- Watch out for unusual cookies. Cookies are small pieces of data that websites share with your web browser. Some cookies are used to analyse how you interact with the website, while others are used for authentication purposes, security measures, or targeted ads. If you don't want third parties to develop a profile about your online and offline activities, look out for cookies that track your location, purchase history, and search history.
- Pay attention to who has access to information about you. If an organisation's website is tracking your information and the organisation isn't careful about who they sell the collected data to, the organisation could put you at risk of cyberattacks. When you create an account or use a service, read the organisation's privacy policy to learn what personal data will be collected and who your data will be shared with.

- Choose your own settings for data tracking. Most websites will ask you for permission to track your activity through cookies. You can opt-out of or block most third-party cookies. If you want to only allow certain permissions, you can adjust your web browser's settings.

Avoid Oversharing on Social Media

Social media can be used to update friends and family about your life, but cybercriminals can also use your accounts as an easy source of information. Follow these tips when using social media:

- Guard your personally identifiable information (PII) by limiting what information you share online.
- Check your privacy settings to minimise the information that can be viewed by the public, especially if you use your real name or the same alias across multiple websites. Cybercriminals can scour the internet for any information associated with your name or accounts.
- Watch out for subtle methods of information gathering, such as quizzes that ask for personal details like your mother's maiden name or your date of birth. Over time, cybercriminals could collect enough details to hack your accounts or steal your identity.

Remember that you are an important part of your organisation's human firewall. Make sure to use strong passwords, use multiple layers of security, and be aware of what data you share and who you share it with. If your personal information is ever shared in a data breach, make sure to quickly change your passwords and reach out to your IT team for guidance. Stay safe!

The KnowBe4 Security Team
KnowBe4.com