KnowBe4

How to Keep Your Organization Safe in and Out of the Office

Whether you work from home or work in an office, the security of your organization must be one of your top priorities. While these two locations can feel quite different, you can use the same precautions no matter whether you're working from the office or at home. Let's look at some important cybersecurity rules and how they can be used both in the office and when you are working at home.

Only Use Secure Devices

- Remember that your device is only as secure as the apps that are running on it. Never install an application or plugin without first checking with your IT department.
- Only use your work devices for work. If you are using your personal computer for work, we recommend that you create a separate user account with a unique username and password.
- In the office, network security is probably managed by your IT department. To help keep your home internet connection secure, use a complex password on your router. If your organization offers access to a Virtual Private Network (VPN), connect to that as well.

Protect Your Physical Workspace

- In the office, watch out for piggybacking and tailgating. A piggybacker is someone who claims to be part of your organization and follows you into a secure area without the use of a badge or entry code. A tailgater is someone who waits for you to enter or exit a secure area and then sneaks in while the door is still open. Be suspicious of anyone who you do not recognize and don't be afraid to ask for identification.
- At home, find a private and comfortable workspace, where no one can view your screen while you work. You must keep all sensitive information out of sight for any unauthorized persons, including your partners, children, and friends.
- Always lock your computer when you step away from your desk. If you leave your computer unlocked, anyone can use it to access sensitive data, steal your login credentials, or even install malware.

Think Before You Click

- Never click a link or download an attachment from an email that you weren't expecting. Even if the sender appears to be part of a legitimate organization, the email address could be spoofed.
- When an email asks you to log in to an account or online service, navigate to that service through your browser. Never click the link in the email. Navigating to the site directly ensures that you're logging in to the real website and not a look-alike site.
- When in doubt, call the sender of the email to be sure the request, link, or attachment is legitimate. Do not call the phone number provided within the email as it may be a fake number.

The KnowBe4 Security Team