Cybersecurity in the

Home Office

Creating a culture of cybersecurity from your home office to the board room is a responsibility shared among you and your colleagues. Here are simple tips to help secure your home office. Many of these tips also apply to your workplace.

Security Tips for Working from Home (WFH)

Shred it: It is best to avoid printing or writing down sensitive information when working away from the office. If this is unavoidable, make sure to either cross-shred the documents or bring the sensitive information to a workplace shred bin.

Cover it: If your work equipment has a camera on it, cover it when not in use to protect your privacy. A sticky note works well for this.

Lock it: Lock your workstation when you walk away. If you are at a location other than your home, make sure not to leave your computer unattended. Additionally, do not allow others to use your work computer, including family members, friends, or children.

Protect it: Make sure your home Wi-Fi network requires a hard-to-guess, unique password and uses WPA2 or WPA3 options. Consider replacing your wireless router if it does not support WPA2 or WPA3. Contact your internet provider and ask if you are not sure.

Connect it: If a device connects to the cloud or is accessible online, it likely has a default password. One of the most important steps to protect these devices and your home network is change the default password. You do not want a hacker logging in and exploiting home security footage. If multi-factor authorization is an option – use it.

VPN it: When away from the office, use VPN. There are many benefits to doing this including an encrypted connection to your company network, receiving up-to-date patches and the ability to change your company passwords remotely.

Follow these Security practices:

Log off your computer when you are done using it – especially at the end of the day.

Lock your computer when you walk away from it.

Do not send company data to your personal email accounts.

Never download data onto an external memory stick or upload to a cloud storage service not approved by your company.

Only log on to VPN over a secure Wi-Fi network – public Wi-Fi spots cannot be trusted to keep information confidential.

SECURE

If you are sending or replying to an email with confidential data use your workplace protocols to send securely.

Don't use your smartphone to take pictures of your workspace or company documents.

Never share your password with anyone.

First Midwest Bank

A division of OLD NATIONAL BANK

Member FDIC

EQUAL HOUSING LENDER