

Staying Cybersafe While Working Remote



BE AWARE

Cybercriminals will try to exploit people's curiosity and trust, especially during times of disruption.

Phishing attacks are on the rise. Do not open attachments or click links from unknown or unexpected sources. Never give away your credentials.

Work-From-Home situations present an extra need for caution.

Mobile devices are also a target of cybercriminals and need to be secured.

Things to DO

Protect GBX Data & Equipment

- Always consider the general rule of “Need to Know” before sharing sensitive data.
- Never save sensitive company data to personal devices.
- Always use caution when browsing, clicking on links, or opening attachments.
- Always roll over links before clicking to validate the destination.

Protect your home network

- Ensure home network firewalls and **Wi-Fi security** are enabled.

Protect your Mobile device

- Load new apps only from trusted sources.
- Secure your mobile devices.

Things **NOT** to DO

DON'T share passwords, credentials or company devices with anyone. Not even family members.

DON'T take office equipment home without informing the Help Desk.

Maintain updated AntiVirus protection

Free Sophos licenses are available to GBX employees for personal use on up to 10 devices.

<https://home.sophos.com/en-us/employee/greenbrier.aspx>

Questions? Email corporateitsecuritygroup@gbrx.com