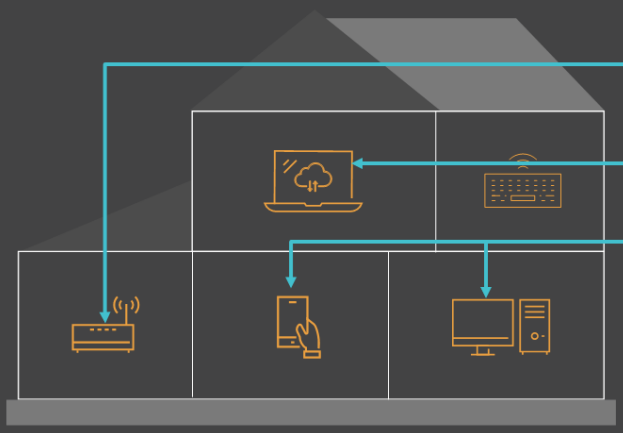
Maintaining a safe work from home environment

mspLOGO

1. First, make sure your WiFi and home network is safe and secure:



- [ ] Make sure you have a strong password on your WiFi network
- [ ] Make sure your router's administration page has a password as well
- [ ] Turn on "Automatic Firmware Updates" on your router to keep it secure
- [ ] Separate your work system from other devices if possible(on a password protected Guest Network) or ensure you are always using the VPN(if you are using one)
- [ ] Update other devices and applications that are in use on your network

Tip: If you need assistance securing your router, let us know. We want to make sure your environment is a safe as possible

2. Second, ensure you are using your work device in a secure manner:

- [ ] Make sure you have a "work only user" with a strong password
- [ ] Log out of the user account when it is not being used for work
- [ ] Don't share your work computer with others if possible
- [ ] If you are using remote access tools or a VPN, make sure to disconnect from it when not in use
- [ ] Avoid checking personal email or doing personal business on the work system
- [ ] If you are using your own system for work, check for updates regularly for the operating system and programs that are running on your work system (if you are using a work laptop, we already have this covered for you).
- [ ] Update any Antivirus/Endpoint Security products and make sure all features are turned on (if you are using a work laptop, we already have this covered for you)

3. Finally, use secure practices when receiving emails or links to external websites:

The amount of phishing, malware, and fake sites has increased dramatically as bad actors focus on the COVID-19 threat, pretending to offer information about:

- Infected people in your area
- Health Guidance – pretending to be Government organizations
- Offering testing in your area or masks and other protective gear
- Pretending to be someone in your business with important information or an invoice to pay
- Links to documents, news articles, or sensational headlines

During these times, it is important to be aware of the additional risk that is presented. Here are some clues to look out for in emails you receive.

- Spelling errors or poor grammar
- High sense of urgency or immediate calls to action
- Shortened links that don't show you where the link takes you
- Unsolicited documents or strangely named attachments
- Links to Office 365/Google Docs documents that ask you for a username and password
- Strange email address in the "From" or "Reply To" fields in the email

If you receive a suspicious email from someone in your organization or a partner/vendor you usually do business with, ask yourself a few questions:

- Is the email from someone I usually receive emails from?
- Is the topic, grammar, and signature consistent with an official communication?
- Do they normally send emails in this way with these types of attachments?
- Does the email address look correct?

If you are not confident that the email or attachment is legitimate, you should contact the sender through other means. Instead of replying to the email, send the person a chat, or call them to verify they sent it.

If the email appears to be from an external government organization, google the site and visit it directly instead of clicking on a link in an email.

What you can do

If the email looks like your company is being targeted, and it is clearly fake, send us a copy to review. This will help us determine whether this is just a one-off spam email, or something we should notify the entire company to look out for.

If you mistakenly clicked on a link or opened an attachment, let us know as soon as possible. Then we can determine the next steps to ensure data is protected.

www.website.com

email@email.com

(123) 456-7890