


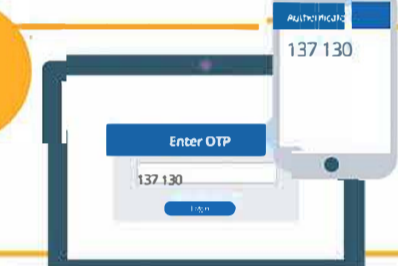



10 Tips to Work from Home - SECURELY


1  **Phishing scams are rife.** Be aware of phishing scams targeting remote workers with sensational or emotional messages. Without your colleagues around, you need to be extra vigilant of both email and phone scams. Report any suspicious messages to your IT Security team.


2  **Be extra careful of fake news and malicious websites taking advantage of newsworthy events, such as the COVID-19 pandemic.**

3  **Your passwords are the key to the kingdom.** Without the company network to protect you, the power now lies squarely in your hands, or your passwords. Make sure your password for each critical site is strong and unique. Check the policy on password managers and use one if allowed.


4  **Use Multi-Factor Authentication** wherever possible. This is combining your username and password with something that you own, such as a One Time Password app on your phone.

5  **Don't fall for "credential phishing" attacks,** where scammers trick you to hand over your username and passwords. Best is to not ever click on links asking you to update details. Rather bookmark the sites you frequently visit.


6  **Apply all basic security features.** Keep your operating system, plug-ins and anti-virus software up to date and apply security patches when necessary.


7  **Secure your home WiFi Network.** There are 2 basic must-dos to set this up securely: Change your default router password. If you're still using "admin/admin," "admin/password" or something similar to log into your router itself. Change that.

Next, when setting up a password for your WiFi network, make sure you choose WPA2. And whatever you do, do not run a wifi network without a password.

8  **Keep your work environment private.** Keep your home environment safe and ensure nobody is allowed to access your work computer, including your family and kids. Others could unintentionally download malicious software or access files they shouldn't see. Ensure that your work conversations remain private and check your policy on smart home devices like Alexa or Google Home

Avoid printing at home, and if you must, make sure you lock sensitive documents away and shred them before discarding them.

9  **Use a VPN.** Using a virtual private network (or VPN) provides a secure tunnel for all your internet traffic, preventing criminals from intercepting your data... Ask your security team to set one up for you

10  **Read your policies.** They are there to keep you, the company and our data safe. In turn, this allows you to work in the comfort of your PJ's and slippers. You are our strongest line of defence so remember to remain super vigilant

Thanks for keeping your organisation safe while working remotely