Cybersecurity during Covid-19

Ten security considerations for working-from-home

May 2020

As Covid-19 turns working-from-home into the new normal, adapting and keeping a focus on cyber security in all settings, is critical. Here is what you can do have more securely work-from-home configuration.

1. Secure your environment

Try to designate a room as your home office, lock the door if you can. Ensure private conversations remain private by turning off Alexa and Google Assistant.

2. Maintain a clear desk policy

Make certain all paper copies of sensitive information are stored out of sight and secure when not in use. If possible, shred when no longer needed.

3. Lock screens

Lock screens when not in use and shut down devices when the working day is over. Don't leave laptops in plain sight unattended.

4. Set strong passwords

Secure your work device with strong passwords, consider using a password manager.

5. Keep work and home devices separate

Don't use work devices to download personal apps or conferencing tools without IT agreement. Be disciplined in using personal devices for personal internet browsing.

6. Connect via VPN

Always connect through a VPN to ensure your internet connection is encrypted and your information and online activity are secure.

7. Be aware of your privacy

Keep privacy screens on and be mindful of what's in the background of your webcam. Confirm you know who's attending your conference calls.

8. Secure Wi-Fi access points

Verify wireless routers use WPA2 and that they're protected with strong passwords; change the standard admin passwords.

9. Be aware of Covid-19 phishing attacks

Organized crime groups are exploiting the current concerns over COVID-19 to target for a range of scams.

Look out for emails that:

- Start with a generic greeting like "Dear Colleague".
- Have poor grammar or spelling mistakes.
- Solicit personal or financial details.
- Offer a cure or test for the virus, or scarce items.
- Demand action with a threat or time imperative.
- Ask for charitable donation via unusual channels.

10. What to do if you clicked on a suspicious link?

Don't panic and follow these steps:

- Open your antivirus software, and run a full scan. Carefully follow any instructions given.
- Contact your IT department to talk you through what you need to do next.
- If you were tricked into providing your password, change your password immediately.

Tareq Dreiza
Head of Technology
KPMG in Saudi Arabia
E: tdreiza@kpmg.com
T: +966 55 388 9928

Ton Diemont
Head of Cybersecurity
KPMG in Saudi Arabia
E: antondiemont@kpmg.com
T: +966 56 860 8393