



COVID-19

10 security considerations for working from home

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's what you can do to work-from-home more securely.

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 ensure they're protected with strong passwords.

9. Be aware of COVID-19 phishing attacks

Organized crime groups are exploiting our concerns over COVID-19 to target us 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 anti-virus 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.
- Change your password immediately if you were tricked into providing your password,

Contact

David Ferbrache,
Global Head of Cyber Futures

KPMG International

T: +44 203 920 0492

E: david.ferbrache@kpmg.co.uk

home.kpmg

home.kpmg/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Evalueserve.

Publication name: COVID-19

Publication number: 136906-G

Publication date: April 2020