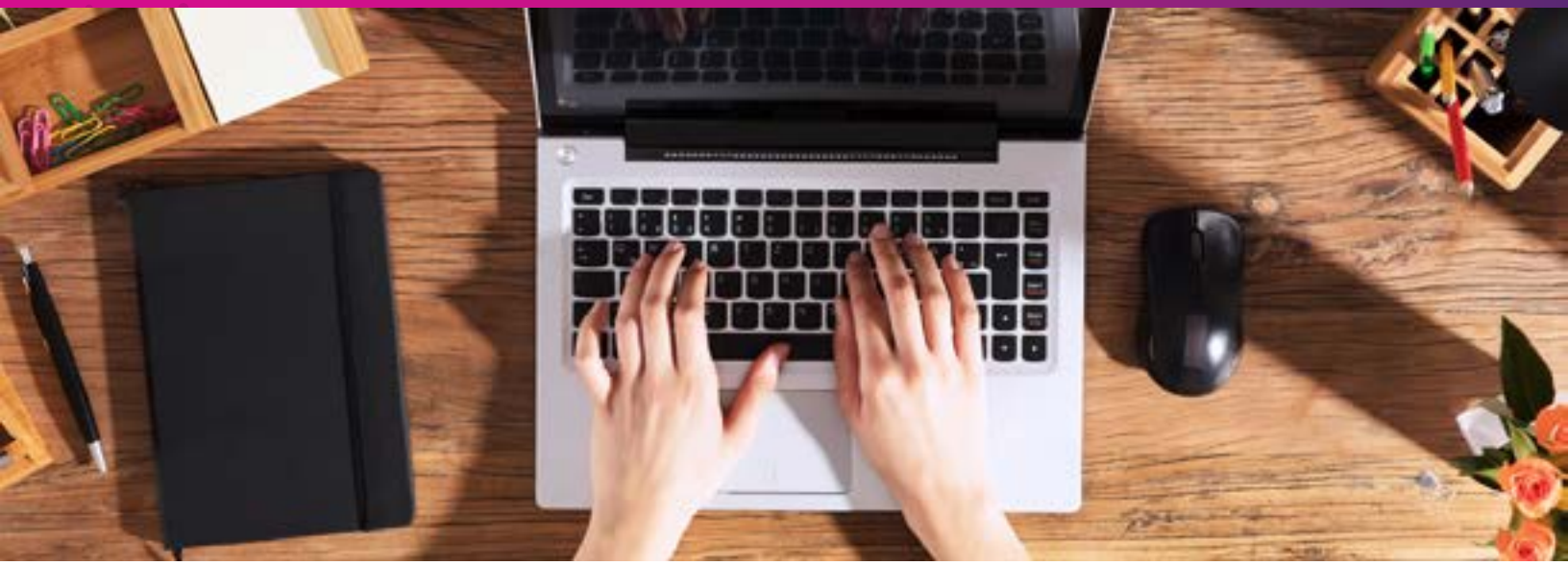
Security Checklist for Remote Work

Insight



A practical guide for teammates and IT professionals

The rapid rise of remote work also creates abundant security vulnerabilities. But defending company data doesn't rest with one team. Effective security requires vigilance and cooperation across the organization — from the IT department to the end user.

Remote user endpoint protection

Recommendations for remote workers

- ☐ **Reboot your desktop or laptop daily.**
  A reboot wipes away the current state of the software, including any problems that have developed, and allows it to start over from square one.
- ☐ **Reboot your home router and/or cable modem weekly.**
  Experiencing slow Wi-Fi? Routers are like computers and can run out of memory. During a reboot, routers can get a fresh start and also find channels with lower traffic.
- ☐ **Optimize your bandwidth.**
  Limit activity on your network (such as streaming services) while you're trying to run a video conference. Also, lessen work for your computer by closing excess apps or browsers.

Recommendations for IT

- ☐ **Make Two-Factor Authentication (2FA) mandatory for all remote workers.**
  1. Include 2FA for email and to access critical systems or applications.
  2. Ensure you have backup codes in case 2FA doesn't work.
  3. Use an app for 2FA rather than SMS.
- ☐ **Ensure all mobile equipment has hardware encryption** (where not possible, software encryption is ok).
- ☐ **All mobile devices must have full disk encryption.**
- ☐ **If you are renting devices, ensure that you wipe the hard disks** before returning them to ensure no residual data is left behind.

- ☐ **Mobile devices are now business-critical machines** and must be subject to the same stringent policies, such as software updates, backup and protective controls.
- ☐ **Monitor endpoints** (laptops, wireless printers, etc.) more closely and, if possible, **use Endpoint Detection & Response (EDR) tools.**

Top security threats

- 55% phishing emails
- 32% malicious websites purporting to offer helpful information about the pandemic
- 28% increase in malware
- 19% increase in ransomware attacks[1]

Cybersecurity

Cyber criminals are out to exploit remote workers. Home Wi-Fi networks have weaker protocols than office environments, making it easier for hackers to access the network traffic. 71% of IT and security professionals globally report a spike in security threats or attacks since the expansion of work-from-home.[1]

▶ Reminders for employees

- ☐ **Change your home Wi-Fi password.**
- ☐ **Don't allow others (kids, family members) to use your work devices.**
  1 in 5 people have shared their work device password with a family member.[2]

- ☐ **Don't install unauthorized software or apps.**
  1 in 3 people have downloaded an app on a work device without approval.[2]

- ☐ **Keep all devices (corporate and personal) up to date** with the latest software and operating systems.
- ☐ **Use a validated VPN solution** for secure network access.
- ☐ **While using the internet, be cautious of pop-ups reporting computer virus warnings. Do not click them.** If you suspect your computer is infected, contact IT immediately.

▶ Reminders for IT

- ☐ **Reinforce the need to protect confidentiality to employees.**
- ☐ **Remind employees that you are monitoring their activity** as per your policies and terms and conditions of employment.
- ☐ **Notify teammates of software or operating system updates** and provide instructions on how to complete the update.

Contact IT immediately if you experience:

1. Loss of control of keyboard or mouse
2. Slow-down of computer performance
3. New apps you didn't install
4. Strange pop-up windows

Phishing emails

▶ Be an active defender.

- ☐ **Are there spelling or grammar mistakes?**
  You should also look for unusual spacing or formatting.
- ☐ **Look for inconsistencies.**
  - Does the sender's tone or language match what you've come to expect from that colleague?
  - Call the sender to verify the email is legitimate.
- ☐ **Remember, phishing emails consistently make it past technical controls.**
  Attackers are constantly evolving their techniques to disguise malicious links.

▶ Reminders for employees

- ☐ **Be on alert for phishing emails** and other attempts to compromise/steal account details.
- ☐ **Assume email attachments from contacts outside your company** are suspect and use caution.

- ☐ **Report any suspicious emails to IT.**
- ☐ **Report malware/ransomware infections immediately.**
- ☐ Trust your gut. If everything in the email seems ok but you're still not sure, **call the sender to verify the email or report it to IT.**

▶ Tips for IT

- ☐ **Create and/or educate employees** on the process for reporting suspicious emails.
- ☐ **Deploy phishing email tests** to ensure employees are remaining vigilant and following reporting protocol.
- ☐ **Consider disabling email forwarding** for all accounts or set up an alert if email forwarding is switched on.
- ☐ **Caution employees about remote helpdesk calls** purporting to be from Microsoft or other computer vendors.
- ☐ If relevant, remind employees that **critical internal communications only come from a specific email**, such as hr@someone.com and to **check sender emails carefully.**
- ☐ **Let employees know it's ok to make a mistake and to notify IT** if they accidentally click on a suspicious link or open a potentially harmful document.

Video meetings and calls

▶ Reminders for employees

- ☐ **Only use company-approved conferencing and collaboration solutions.** If you are creating a meeting with someone outside of your company, offer to host the meeting to ensure use of your company-approved platform.
- ☐ **Set a password for online meetings.**
- ☐ **Don't have confidential calls and business discussions near smart speakers,** such as Amazon Alexa, Apple Homepod or Google Home.
- ☐ During a call, remember to **mute your microphone if you're not speaking.**
- ☐ **When not in use, ensure webcams are blocked by default** (physically and by the conference app you use).
- ☐ **If you record a meeting, all participants must be notified.**
- ☐ **Do not upload company meetings to unapproved cloud storage services or public video services,** such as YouTube or Vimeo.

▶ Tips for IT

- ☐ Communicate to employees about **approved conferencing and collaboration apps.**
- ☐ Educate employees about **basic security and privacy settings.**
- ☐ Ensure that participants **kicked-out of online meetings cannot rejoin.**

Data backup

▶ Reminders for employees

- ☐ **Back up data on an approved external hard disk** that is not permanently connected to the device.
- ☐ **Use only approved cloud storage services (if permitted).**
- ☐ **Contact IT to discuss use of any new cloud storage or cloud service solution before using it.** Cloud services include, but are not limited to:
  1. File sharing
  2. File storage and synchronisation
  3. Project management apps
  4. Collaboration tools
  5. Note taking and storage
  6. Photo storage and sharing

▶ Tips for IT

- ☐ **Provide employees with software** to ensure their critical documents are backed up properly.

Sources

[1] Check Point. (May 2020). "A Perfect Storm: the Security Challenges of Coronavirus Threats and Mass Remote Working."
[2] OneLogin. (2020, May 7). "World Password Day Survey: Global Remote Workforce"