# 7 SECRETS AND LIES

## of Remote-Work Cybersecurity

Experis® ManpowerGroup

When was the last time you changed the password on your home router?

01

## BRING YOUR OWN DEVICE (BYOD)

Whether employees use locked-down laptops and phones provided by their companies or not, they still use their home wi-fi, their router, their printer...

All these devices could **open doors to cyber criminals** targeting remote workers.

02

## COMMUNICATION TOOLS LIKE *ZOOM* AND *TEAMS*

New entry-points for hackers.

**TIPS**

- **Update** to latest version
- **Filter** participants
- Use **waiting rooms**
- **Mute** participants
- **Disable** participants' cameras and the "join before host" feature
- **Set strong passwords and Restrict** the "record" function

03

## ANTI-VIRUS

- Anti-viruses can only protect you from known viruses.
- Firewalls can't scan encrypted traffic.
- "The cloud does not exist". It is just someone's computer connected to the internet.

Backups are always a good idea. Although recent strains of ransomware (e.g. Maze) steal your data and then encrypt it.

04

## VPNs YOU'RE NOT SAFE

- Avoid connecting to public Wi-Fi networks if possible. Especially those that block VPN connections.
- Choose your browser carefully.
- Always buy and download (personal) VPN software from authorised websites or vendors.
- Privacy and logging: Be careful of where your VPN datacenter really is located.

05

## PASSWORDS ARE A KEY FACTOR

my dog loves squirrels

Set strong passwords.

**********

Activates the encryption features.

06

## YOUR TEAM YOUR STRENGTH

Communication is key.

Is it important to train and up-skill my employees?

Yes,

but continuously, using relevant and updated content.

- Educate them about company policy.
- Measure their effectiveness.

07

## RANSOMWARE

Ransomware is malicious software that can encrypt your systems and require payment of money to restore system functionality.

- Keep your **Software updated**.
- **Know** exactly what **phishing** looks like.
- Keep your **Antivirus and Firewall updated**.
- **Backup and test your backups** regularly.
- **Limit user privileges** to the minimum needed.
- When your employees leave your company, **remove them from the system ASAP.**
- **Segregate** both your **network and backups.**

If you take these tips into account, you will **make the path more difficult for cybercriminals**, but as you know, their attacks evolve very quickly.

If you need to protect the information of your company, customers and employees, in Experis we have developed simple and effective solutions to help you overcome the challenge of Remote-Work Cybersecurity.

**Get to know them at** Experis.co.uk/cyber-risk-service

Experis® ManpowerGroup