Physical protection of data and devices

There's a physical side to practising good cyber security. Here are some tips to help you protect yourself and your data from being compromised.

What should you do?

Always lock devices when unattended.

A few minutes could be all it takes for a threat actor to access what they need.

Make sure you aren't tailgated into secure areas.

Be aware of who might be loitering around secure areas at your workplace and report it to your building security team if they appear to be suspicious.

Be mindful of what you talk about in public.

Work conversations in public shouldn't include highly sensitive or private information.

Secure your removable media.

Removable media can introduce malware and enable accidental or deliberate exporting of sensitive data. Avoid this risk by never connecting unknown USBs or external hard drives to your work or personal devices.

Turn off bluetooth.

In public, disable your bluetooth when it's not in use and be aware of all devices you are pairing with.

Watch out for shoulder surfers and reflections in windows.

While working or entering sensitive information, be mindful of what may be visible to someone near you.

Cover or unplug your webcam.

When you are not in a meeting, cover your webcam. In some cases, webcam recordings taken without knowledge of the user have been used in extortion attempts.

Be mindful of QR codes.

It is quick and easy for criminals to create QR codes and replace them in restaurants and other businesses as part of attempts to obtain your personal information. Check the URL displayed first and if it looks suspicious, don't click.