FACT SHEET

Shred-it's Guide to Resuming Data Security After Summer Holidays

During the summer months, employees take well earned annual leave. However, when they return, it's a good idea for businesses to remind employees on how to deal with confidential information to reduce their risks of a data breach.

DID YOU KNOW... The average cost of a data breach is SGD 4,934,070? [1] And that 31% of consumers would lose trust in a company that experiences a data breach? [2]

Here are some of the best ways employees can utilise data security best practices following summer annual leave, during work trips and when working remotely:

1. **Minimise the amount of information stored on a mobile device** to only what is needed for work.
2. **Be alert when working remotely** in a coffee shop, airport lounge, or bus. Put away work or change seats if anyone acts suspiciously.
3. **Avoid sharing electronic devices with family, friends, and other visitors.** Lock away when they are not being used. Keep sensitive and confidential papers in a secure place too.
4. **Watch out for phishing emails and malicious websites.** Signs include spelling and grammar mistakes, suspicious email addresses and urgent calls-to-action. Never send personal details such as names, address, and credit card details over email.
5. **Follow company procedures for secure disposal of digital and paper information.** Do not put paper into bins or recycling containers. Do not simply bin or recycle end-of-life electronic devices. Bring them to the office for secure disposal after the summer period.
6. **Do not use unknown USB devices.** Only use company-approved devices.
7. **Never leave mobile devices unattended** in public or visible in a locked vehicle.
8. **Update software and install patches immediately.** Research has shown that 82% of discovered breaches occurred due to a failure to update software patches. [3]
9. **Strengthen passwords on all devices and accounts** (long string of characters, incorporating numerals, letters, and symbols). Over 60% of breaches attributed to leveraged credentials. [4]
10. **Turn off Wi-Fi and Bluetooth connectivity when not being used.** To transmit anything confidential or connect to the office, use personal hotspots, a virtual private network (VPN) or password-protected Wi-Fi networks. Connecting by Bluetooth encrypts data.

[1] https://www.ibm.com/security/data-breach
[2] Shred-it Data Protection Report 2020
[3] Voke Media, Secure Operations Automation Market Snapshot report
[4] https://www.verizon.com/business/resources/reports/dbir/

To learn more about best practices to stay seasonally secure, visit shredit.sg or call 6787 7777.

We protect what matters.

Shred-it®
A Stericycle® Solution