INFORMATIEBLAD

De gids van Shred-it voor het hervatten van gegevensbeveiliging na de zomervakantie

Tijdens de zomermaanden nemen werknemers welverdiende vakantiedagen op. Wanneer ze terugkeren, is het echter een goed idee voor bedrijven om werknemers eraan te herinneren hoe die met vertrouwelijke informatie moeten omgaan, om de risico's die ze lopen op een datalek te verkleinen.

WIST U DAT ... De gemiddelde kosten van een datalek €3,533,430?[1] En dat 31% van de consumenten het vertrouwen zou verliezen in een bedrijf dat te maken krijgt met een datalek? [2]

Hier zijn enkele manieren waarop werknemers na de zomervakantie hun voordeel kunnen doen met best practices op het gebied van gegevensbeveiliging.

1. **Minimaliseer de hoeveelheid informatie die op een mobiel apparaat wordt opgeslagen tot** alleen wat nodig is voor het werk.

2. **Wees alert wanneer u op afstand werkt** in een koffiebar, luchthavenlounge of bus. Berg uw werk op of wissel van stoel als iemand zich verdacht gedraagt.

3. **Vermijd het delen van elektronische apparaten met familie, vrienden en andere bezoekers.** Berg ze op als ze niet worden gebruikt. Bewaar gevoelige en vertrouwelijke documenten ook op een veilige plaats.

4. **Pas op voor phishing-e-mails en kwaadaardige websites.** Waarschuwingssignalen zijn onder meer spel- en grammaticafouten, verdachte e-mailadressen en dringende oproepen tot actie. Verstuur nooit persoonlijke gegevens zoals namen, adres en creditcardgegevens via e-mail.

5. **Volg de bedrijfsprocedures voor veilige verwijdering van digitale en papieren informatie.** Gooi geen papier in bakken of recyclingcontainers. Gooi elektronische apparaten aan het einde van hun levensduur niet simpelweg in de vuilnis- of recyclingbak. Breng ze na de zomerperiode naar kantoor om ze veilig af te danken.

6. **Gebruik geen onbekende USB-apparaten.** Gebruik alleen apparaten die door het bedrijf zijn goedgekeurd.

7. **Laat mobiele apparaten nooit onbeheerd achter** in het openbaar of zichtbaar in een afgesloten voertuig.

8. **Installeer software-updates en patches onmiddellijk.** Onderzoek heeft aangetoond dat 82% van de ontdekte inbreuken plaatsvond als gevolg van het niet installeren van software-updates en patches.[3]

9. **Versterk wachtwoorden op alle apparaten en accounts** (lange tekenreeks, inclusief cijfers, letters en symbolen). Meer dan 60% van de inbreuken wordt toegeschreven aan benutte inloggegevens. [4]

10. **Schakel wifi- en Bluetooth-connectiviteit uit wanneer ze niet worden gebruikt.** Gebruik persoonlijke hotspots, een virtueel particulier netwerk (VPN) of met een wachtwoord beveiligde wifi-netwerken om vertrouwelijke informatie te verzenden of verbinding te maken met het kantoor. Door er verbinding wordt gemaakt via Bluetooth, worden gegevens versleuteld.

[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/

Ga voor meer best practices om uw veiligheid te garanderen naar shredit.nl of bel 0800 0114.

Wij beschermen wat van belang is.

Shred-it®
Een Stericycle®-Oplossing