Higiene Digital Parte 3:

A Regra do "Atraso na Partilha" e o Perigo do Wi-Fi Público

Janeiro 2026 | Parte III

A urgência em mostrar onde estamos ou a facilidade de ligar o portátil a qualquer rede disponível são as maiores brechas de segurança para quem trabalha em mobilidade.

- Não publique a sua localização em tempo real (ex: Stories no Instagram num evento ou restaurante).
- **Conselho:** Partilhe o que fez, não o que está a fazer. Isso evita que saibam que a sua casa ou escritório estão vazios e protege a sua rotina.

Criminosos utilizam geolocalização para saber que a sua infraestrutura física está mais vulnerável ou para lançar ataques de engenharia social ("Olá, vi que estás na conferência X, podes confirmar este documento?").

Publique as fotos apenas quando já tiver saído do local. O impacto do marketing é o mesmo, mas a segurança é muito superior.

Usar um Wi-Fi público é como ter uma reunião confidencial no meio da rua aos gritos.

- Um atacante pode criar uma rede com o nome "Wi-Fi_Aeroporto_Gratis". Ao ligar-se, tudo o que escreve (passwords, e-mails, dados bancários) passa pelo computador dele antes de chegar à internet.
- **O nosso conselho:** Use sempre os dados móveis (Hotspot do telemóvel) ou uma **VPN empresarial** configurada profissionalmente.

A TEC2iT® protege a sua mobilidade

Através de:

- Implementação de **VPNs seguras** para acesso remoto a servidores.
- Configuração de **Redes de Convidados (VLANs)** isoladas na sua empresa.
- Segurança de terminais e dispositivos móveis.

A sua equipa viaja em trabalho? Garanta que os dados da empresa não ficam pelo caminho.

Fale connosco para uma auditoria de redes e acessos remotos.

Figura 1: Usar um Wi-Fi público é como ter uma reunião confidencial no meio da rua aos gritos.