Higiene Digital Parte 2:

O Perigo do "Oversharing" e a Exposição Corporativa

Janeiro 2026 | Parte II

Muitas vezes, a maior vulnerabilidade de uma empresa não está na firewall, mas na página "Sobre Nós" do site ou no perfil de LinkedIn dos colaboradores.

O excesso de partilha (Oversharing) é o combustível para ataques de engenharia social.

Colocar a foto de rosto (tipo passe) + e-mail direto + o cargo de cada colaborador no site parece sinal de transparência e profissionalismo.

No entanto, para um atacante, isto é um kit completo de personificação.

Como o ataque acontece:

Recolha de Biometria: Fotos em alta resolução são usadas para criar perfis falsos em apps de mensagens (WhatsApp/Teams). O atacante usa a sua cara para pedir uma transferência urgente a um colega.

Se o atacante sabe quem é o contabilista ou o RH, ele envia "faturas falsas" ou "currículos com vírus" diretamente para o alvo certo.
Endereços escritos em texto simples no site são capturados por bots em segundos e incluídos em listas globais de spam e ataques de força bruta.

O nosso Conselho:

Proteja a sua equipa sem perder o lado humano.

Substitua e-mails diretos por formulários. Evita a recolha automatizada por bots.

Use fotos de equipa contextuais. Em vez de retratos individuais isolados, use fotos em ambiente de trabalho. É mais difícil para uma IA "recortar" e clonar o rosto.

Para o público externo, use geral@ ou comercial@.

Guarde os e-mails nominais para comunicações internas e clientes estabelecidos.

Lembre-se:

Um atacante não precisa de invadir o seu servidor se conseguir convencer um colaborador de que é "o chefe" a pedir um favor.

A sua empresa está demasiado exposta?

Na TEC2iT®, ajudamos a auditar a vossa presença digital e a implementar políticas de segurança inteligentes.

Figura 1: Um atacante não precisa de invadir o seu servidor se conseguir convencer um colaborador de que é "o chefe" a pedir um favor.