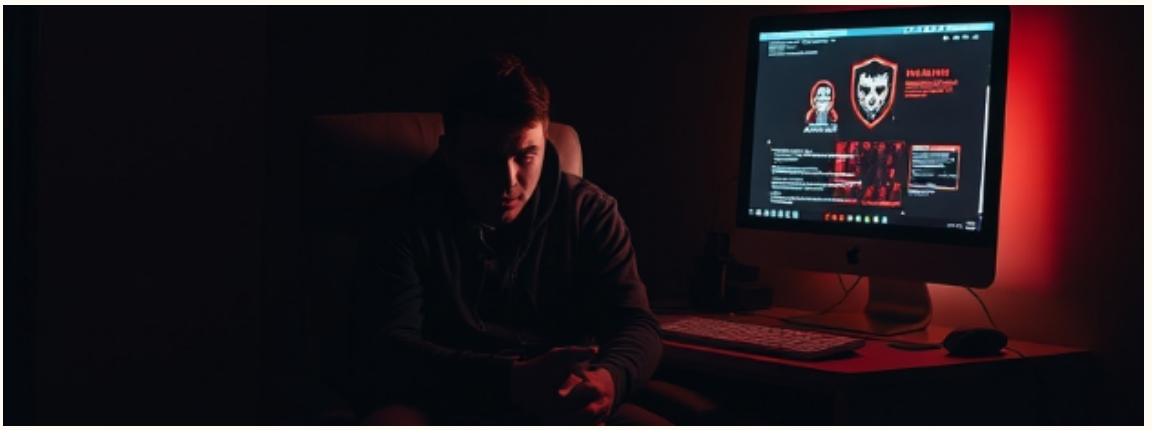
Roubaram meus dispositivos (notebook/tablet/celular), e agora?



Antes de qualquer coisa, temos que avaliar os principais cenários possíveis. O furto, no qual o usuário não percebe imediatamente o ocorrido; e o roubo, que pode acontecer mediante ameaça e violência ou até mesmo sequestro.

No primeiro caso, a proteção regular por senhas fortes, a autenticação de duplo fator e a criptografia são adequadas na maioria das vezes para resguardar suas informações. Já o segundo caso, infelizmente, nos deixa mais expostos às perdas. A vítima em poder dos meliantes é obrigada a liberar acessos a tudo que estiver disponível nos dispositivos, durante o tempo que for necessário para efetivação dos golpes.

Ações desta natureza geralmente envolvem um especialista (hacker) que atua remotamente efetivando as ações nos equipamentos. Focaremos no segundo desdobramento para discutir alguns aspectos de segurança. Com a vítima sendo obrigada a fornecer seus dados e senhas, dificilmente temos como nos proteger de forma 100% eficaz. Algumas medidas, contudo, podem minimizar as perdas, tanto pessoais quanto corporativas.

♦ Mantenha os limites de seus cartões de crédito e PIX os mais baixos possíveis. Não se trata dos limites configuráveis pelos apps, que podem ser aumentados rapidamente, mas sim do limite geral;
♦ Para sistemas corporativos, o fluxo de trabalho (workflow) deve prever limites e alçadas apropriados, preferencialmente com duas ou mais etapas e/ou assinaturas;
♦Mantenha sempre ativado o recurso de rastreamento / localização / reset remoto de seus dispositivos (PCs e dispositivos móveis);
♦ Não salve senhas em nenhum aplicativo. Após o ocorrido, os meliantes podem vasculhar os dispositivos em busca de informações e acessos adicionais.

Se possível, mantenha um celular exclusivo em local seguro para dados e acessos sensíveis. No celular do dia-a-dia, use um único aplicativo bancário de uma conta com saldo e limites financeiros mais restritos possíveis. Uma nova conta em *fintecs* (NuBank, Banco Inter etc.) pode ser aberta com esta finalidade. Certifique-se que nenhum aplicativo neste celular (ex.: Mercado Livre, Shopee etc.) tenha informações sobre outros cartões de crédito ou bancos!

Algumas medidas a serem tomadas assim que possível após o incidente:

- Dispare o reset remoto dos dispositivos.
- Tome as medidas apropriadas (ocorrência policial, acionamento de seguro etc.).
- Altere todas as suas senhas, pessoais e corporativas. É conveniente manter uma listagem atualizada de todos os serviços e aplicativos (sem as senhas!) para agilizar este processo.
- Notifique todas as instituições eventualmente envolvidas, tais como bancos, operadoras de telefonia, empregador etc.

- Notifique todos os seus contatos e solicite a exclusão de grupos de mensagens.
- Cancele certificados digitais pessoais e corporativos.

Observe que são recomendações básicas, as medidas mais apropriadas para cada indivíduo dependem bastante dos programas e dados existentes nos dispositivos.

At.,
Nilton Teixeira
https://www.advancegroup.com.br
Microsoft Partner ID 3288934
Segurança nunca é demais!

ADVANCE GROUP
BECAUSE IT MUST BE A SOLUTION