BOLETIM DE SEGURANÇA DA INFORMAÇÃO # 3

USO SEGURO DE DISPOSITIVOS MÓVEIS

Celulares, tablets e computadores fazem parte do nosso dia a dia. Com eles, acessamos bancos, redes sociais, mensagens, fotos, documentos e, muitas vezes, também sistemas e informações de trabalho.

No entanto, é importante deixar claro: **o uso de dispositivos pessoais para atividades no ambiente do nosso trabalho não é a prática mais recomendável do ponto de vista da segurança da informação**. Sempre é melhor utilizar os equipamentos especialmente da nossa instituição pois eles são configurados, monitorados e protegidos especificamente para o ambiente de trabalho.

Mesmo assim, sabemos que, na prática, muitas pessoas acabam utilizando seus próprios celulares e computadores para acessar e-mails, documentos e sistemas da empresa. Quando isso acontece, o cuidado precisa ser redobrado, porque **esses dispositivos deixam de conter apenas informações pessoais e passam a armazenar ou acessar dados de outras pessoas do nosso ambiente de trabalho.**

CASO REAL: VÍRUS NO CELULAR

Uma colaboradora utilizava seu **celular pessoal** para acessar e-mails e sistemas da empresa no dia a dia do trabalho. O aparelho também era usado em casa, inclusive por familiares, de forma eventual.

Em determinado momento, o celular foi **comprometido por um aplicativo malicioso**. A investigação posterior indicou que o problema provavelmente começou quando um familiar — possivelmente o filho — utilizou o aparelho para instalar **jogos baixados fora da loja oficial**, sem que a usuária percebesse o risco envolvido.

O aplicativo continha um vírus que passou a capturar informações do celular. Como o dispositivo tinha acesso aos sistemas corporativos, os golpistas conseguiram **obter dados da empresa**, que passaram a ser utilizados em **tentativas de fraude e golpes contra terceiros**.

O incidente gerou um grande transtorno: necessidade de investigação técnica, troca de senhas, revisão de acessos e comunicação do ocorrido. Tudo isso começou com um dispositivo pessoal, compartilhado no ambiente familiar, sendo utilizado também para atividades profissionais.

Esse caso mostra que **o risco muitas vezes não está em uma ação intencional**, mas em práticas comuns do dia a dia, como compartilhar o celular ou instalar aplicativos sem os devidos cuidados.

RECOMENDAÇÕES PRÁTICAS DE PROTEÇÃO

Para reduzir riscos no uso de dispositivos móveis, especialmente quando forem utilizados para atividades profissionais, siga estas orientações:

PROTEÇÃO DO DISPOSITIVO

- Utilize sempre bloqueio de tela (senha, biometria ou reconhecimento facial).
- Ative o bloqueio automático após alguns minutos de inatividade.
- Nunca compartilhe dispositivos usados para trabalho com outras pessoas.

REDES E ACESSO

- Evite acessar sistemas, e-mails ou bancos em redes Wi-Fi públicas.
- Prefira redes confiáveis e protegidas por senha.
- Quando necessário, utilize VPNs autorizadas.

APLICATIVOS

- Instale aplicativos apenas das lojas oficiais.
- Desconfie de aplicativos que prometem vantagens excessivas.
- Revise e limite permissões concedidas aos aplicativos.

ATUALIZAÇÕES E PROTEÇÃO

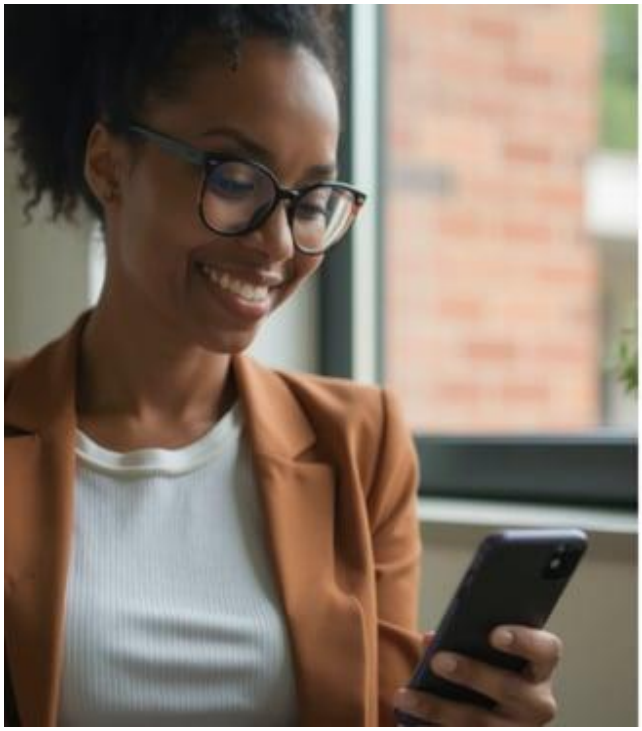
- Mantenha o sistema operacional e os aplicativos sempre atualizados.
- Utilize soluções de antivírus e proteção quando disponíveis.
- Faça backup regular das informações.

CONSCIÊNCIA

- Lembre-se: **seu celular e seu computador também protegem dados de outras pessoas**.
- Um cuidado pessoal ajuda a proteger colegas, clientes e a própria organização.

LINK PARA O VÍDEO

https://vimeo.com/1164708498



Uso Seguro de Dispositivos Móveis