Guia prático elaborado pelo Procon-MG traz dicas de como manter o celular seguro

Você sabia que, entre os anos de 2022 e 2023, mais de 1,9 milhão de celulares foram roubados ou furtados no Brasil? Os dados constam do Anuário Brasileiro de Segurança Pública 2024, publicado pelo Fórum Brasileiro de Segurança Pública, e revelam que, em média, um aparelho foi subtraído a cada 33 segundos no país. Por trás desses números, está um problema ainda mais grave: o uso desses aparelhos para aplicação de golpes digitais que lesam milhares de consumidores. Um celular sem proteção pode ser um atrativo para criminosos.

Veja algumas dicas do Procon-MG

O QUE UM GOLPISTA PODE FAZER SE TIVER ACESSO AO CELULAR

Acessar documentos digitalizados que você possa ter armazenado no celular (cópias de RG, CNH, comprovantes de residência, etc.) e utilizá-los para abrir contas falsas, solicitar serviços, comprar produtos, etc;

Acessar aplicativos de bancos e realizar transferências (Pix, TED, etc.);

Contratar empréstimos ou fazer compras parceladas em seu nome;

Fazer compras online usando cartões de crédito associados a aplicativos ou salvos no aparelho/navegador;

Acessar aplicativos de pagamento (carteiras digitais, PicPay, Mercado Pago) para movimentar dinheiro;

Invadir contas de e-mail (muitas vezes a porta de entrada para redefinir senhas de outros serviços).

Assumir o controle de suas redes sociais (WhatsApp, Instagram, Facebook, Twitter), postar conteúdo fraudulento, aplicar golpes em seus contatos ou pedir dinheiro fingindo ser você;

Acessar serviços de armazenamento em nuvem (Google Drive, iCloud, Dropbox) para roubar mais dados e arquivos;

Usar informações privadas para chantagear e extorquir você, ameaçando divulgar esses dados;

Usar sua lista de contatos para enviar mensagens de phishing, links maliciosos ou aplicar golpes (como o do "novo número") em seus amigos e familiares;

Acessar seu histórico de localização.

DICAS DE PROTEÇÃO DO PROCON-MG

Crie senha forte, com letras, números e símbolos;

Se existente em seu aparelho, utilize biometria ou reconhecimento facial;

Configure bloqueio automático em poucos segundos;

Ative a opção de desligar Wi-Fi, Bluetooth ou dados móveis somente com senha. Isso dificulta que desconectem o aparelho da internet;

Ative a opção de desligar o aparelho somente com senha;

Sempre que possível a autenticação em dois fatores deve ser ativada, pois ela manda um código para seu SMS ou conta de e-mail.

CUIDADO COM O CHIP (SIM CARD)

Ative o bloqueio do chip SIM com um PIN, que é uma senha. Assim, mesmo que coloquem o chip em outro aparelho, ele não funcionará. Isso evita que uma pessoa utilize sua linha para receber links, códigos de autenticação ou acessar seus serviços digitais;

Considere utilizar um eSIM (chip virtual), caso seu aparelho seja compatível. O eSIM não pode ser removido fisicamente, aumentando a segurança. Consulte a operadora para saber mais.

LOCALIZAR, BLOQUEAR E APAGAR DADOS

Ative o recurso de localização do seu smartphone;

Habilite o rastreamento em tempo real;

Descubra como bloquear ou apagar seu smartphone remotamente. Isso é possível na maioria dos modelos;

Esses recursos estão presentes no Android e no iOS.