Como se proteger de ataques ao seu smartphone, WhatsApp e Telegram

Celulares não são propriamente dispositivos seguros. Estão tão ou mais sujeitos a ataques hackers que computadores pessoais. Por estarem 24 horas conectados à internet, sua exposição às ameaças cibernéticas é constante, independente de estarem fisicamente perto de nós.

Nos últimos dias têm saído na mídia notícias sobre ataques a celulares de juízes e promotores, revelando conversas realizadas em aplicativos como o WhatsApp e o Telegram:

> ***Procurador diz ter sido vítima de hacker / O Antagonista***
> ***Hacker diz que acessa 'quem quiser e quando quiser' ao invadir grupo do conselho do MP / O Globo***
> ***'Hackers de juízes não vão interferir na missão', diz Moro ao apontar queda de índices criminais. / O Globo***
> ***PF vê ataque orquestrado em invasão de hackers a celulares da Lava Jato / Folha***
> ***Hackers tentam invadir celular de relator da Lava-Jato do Rio em segunda instância / O Globo***

Como um ataque ocorre?

Acesso físico: com o celular em mãos, um atacante pode obter as informações que quiser ou então instalar programas maliciosos no telefone sem que o dono saiba, possibilitando acesso remoto aos dados, gravação de conversas, etc.
Ataque remoto: a distância, o atacante se aproveita de alguma vulnerabilidade em programas ou sistemas do celular e pode, assim como no caso do acesso físico, instalar algum *malware* para conseguir acesso aos dados.
SIM Swap: é o golpe da moda. Uma pessoa com acesso aos sistemas das operadoras transfere o número associado ao chip da vítima para outro chip dos criminosos. É fácil de perceber, porque o telefone da vítima para de receber e fazer ligações ou se conectar à internet pelo 4G.

Engenharia social: golpistas enganam o usuário para obter os códigos verificadores de instalação de aplicativos, como o WhatsApp e o Telegram.
Protocolo SS7: Ocorre a partir da exploração de vulnerabilidades no protocolo SS7 de sinalização telefônica. Nesse ataque é possível espelhar a linha telefônica de modo imperceptível para o usuário. O celular continua funcionando normalmente, mas a comunicação chega também para os criminosos. Foi utilizado pelos EUA para espionar o governo Dilma.

O que fazer para se proteger?

1. Mantenha o dispositivo e aplicativos sempre atualizados, conforme as recomendações dos fabricantes.
2. Utilize sempre senhas ou padrões seguros para manter o aparelho bloqueado.
3. Habilite a autenticação dupla ou verificação em duas etapas (2FA) para o WhatsApp, o Telegram, serviços de e-mail e qualquer aplicativo que permita o uso desta técnica.
4. Não forneça senhas de aplicativos ou códigos recebidos para autenticação de serviços que você mesmo não tenha pedido. Em caso de dúvida entre em contato com o seu fornecedor.
5. Habilite a função para formatar ou apagar os dados do telefone remotamente, caso o telefone seja roubado ou perdido. Os sistemas iOS e Android permitem a localização e a limpeza de dados de forma remota.
6. Não clique em links suspeitos recebidos por SMS ou qualquer outro aplicativo, incluindo WhatsApp e outros programas de troca de mensagens.
7. Mantenha o seu número de telefone pessoal ou coorporativo em sigilo ou com divulgação controlada. Caso vá fazer uma divulgação, venda ou oferecer um serviço, utilize um número “pré-pago”, descartável, específico para divulgação e realização do negócio.
8. Avalie e gerencie o conteúdo das informações armazenadas no telefone. Qual o risco e dano se houver vazamento dos dados/informações armazenados no telefone?
9. Exclua ou faça backup seguro das informações/conversas que necessitarem arquivamento.
10. Instale aplicativos somente da loja oficial do fabricante do seu dispositivo.
11. Mantenha alerta sobre os locais onde você deixa o telefone, quando este não está em uso.
12. Caso não estejam em uso, mantenha as funções wi-fi e *bluetooth* desabilitadas.

13. Sempre que possível, prefira a rede 4G, evitando conectar-se a redes wi-fi públicas, tais como hotéis, shoppings e restaurantes. Se for preciso usar este tipo de rede, use um aplicativo de VPN.

14. Se seu aparelho for roubado, vendido ou enviado para manutenção, utilize os seguintes cuidados:

a) Em se tratando de um número coorporativo, notifique à sua organização sobre o fato e a autoridade competente, em caso de roubo.

b) Se contas de e-mail, redes sociais, etc estavam ativadas no dispositivo, modifique todas as senhas de acesso.

C) Caso seja possível, realize a formatação do aparelho antes da manutenção/venda, ou utilize o procedimento de formatação remota, caso não tenha mais acesso físico ao dispositivo.

15. Realize a instalação de um antivírus.

Colaboração: Fabrício Lana Pessoa – NSINF / TRE-MG
Juarez de Oliveira – CSINF / TRE-PR

Referências:

https://oglobo.globo.com/brasil/hackers-tentam-invadir-celular-de-relator-da-lava-jato-do-rio-em-segunda-instancia-23727415
https://www1.folha.uol.com.br/poder/2019/06/pf-ve-ataque-orquestrado-em-invasao-de-hackers-a-celulares-da-lava-jato.shtml
https://oglobo.globo.com/brasil/hackers-de-juizes-nao-vao-interferir-na-missao-diz-moro-ao-apontar-queda-de-indices-criminais-23733533
https://exame.abril.com.br/brasil/aqui-e-o-hacker-diz-mensagem-no-grupo-do-conselho-nacional-do-mp/
https://www.oantagonista.com/brasil/procurador-diz-ter-sido-vitima-de-hacker-queriam-que-eu-falasse-mal-da-lava-jato/
https://g1.globo.com/politica/noticia/2019/06/12/hacker-diz-que-acessa-quem-quiser-e-quando-quiser-ao-invadir-grupo-do-conselho-do-mp.ghtml
https://www1.folha.uol.com.br/tec/2019/06/saiba-proteger-seu-whatsapp-de-hackers-e-entenda-como-o-ataque-acontece.shtml
https://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf
https://pplware.sapo.pt/redes_sociais/whatsapp-e-telegram-invadir-conta/