BOLETIM DE SEGURANÇA DA INFORMAÇÃO

Edição 6.2 - Agosto | 2019

Casos de furto de celular e tentativas de hackeamento das contas são cada vez mais praticados. A troca do chip para um outro aparelho pode proporcionar o acesso e posse de aplicativos como o WhatsApp para se entrar em contato com amigos e familiares para, por exemplo, pedir dinheiro se passando pela vítima do golpe. Existem também formas de interceptar conversas em aplicativos como o Telegram e o WhatsApp.

Medidas de Segurança

Prevenção - Com a posse do telefone

- Utilizar código alfanumérico (letras e números) para bloqueio de celular. Padrões de desenho (em Android) ou códigos numéricos como "1234", "0000", ou parecidos, se mostram ineficientes.
- Habilitar a biometria ou senha para todos os aplicativos que suportam tais facilidades, como os aplicativos de banco.
- Utilizar autenticação de dois fatores em todas as contas de redes sociais e serviços de Internet (Facebook, Instagram, Gmail, etc), mas nunca por SMS, pois perderá efeito no caso de roubo do celular.
- Desabilitar as notificações na tela de bloqueio do celular.
- Anotar a marca, modelo, IMEI e número de série do aparelho em algum lugar. Também o PIN e PUK do chip (registrados no cartão do chip).

Mitigação - Após o roubo, furto ou perda do aparelho celular

- Atentar para o fato de que, quanto mais tempo se deixar o chip habilitado, mais tempo haverá para a execução da fraude.
- Ligar para a operadora e informar o ocorrido, para o bloqueio do chip.

Outros alertas e recomendações podem ser encontrados na página da

Comissão de Segurança da Informação na intranet

Entre em contato: csi@tre-go.jus.br