BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 06 – Julho/2020

Como agir para evitar a clonagem de *chip* de celular

A clonagem de *chip* de *smartphone* é golpe comum, atualmente. O criminoso cibernético utiliza técnicas diversas para obter informações que permitam a clonagem desse *chip*. Essas técnicas incluem endereços da *internet* falsos, aplicativos maliciosos, *e-mails* que podem conter anexos suspeitos, e outras, ainda mais sofisticadas.

É possível perceber alguns detalhes que indicam a clonagem do *chip* do seu celular, tais como mensagens da operadora informando que o número do telefone está sendo ativado em outro local, alertas de segurança, dificuldade de enviar *SMS* e de fazer ligação, números desconhecidos em sua caixa, barulhos estranhos durante ligações, e aumento no registro de uso de dados.

Mas, tenha calma, e procure seguir **nossas recomendações**.

1) De posse do telefone:

• anotar — em algum lugar seguro, antes de iniciar o uso do aparelho — marca, modelo, IMEI e número de série do aparelho;
• utilizar senha alfanumérica (letras, números, e caracteres especiais) para bloqueio do celular — padrões de desenho (em *Android*) ou códigos numéricos como "1234", "0000", ou parecidos, se mostram ineficientes;
• habilitar a biometria, ou senha alfanumérica, para todos os aplicativos que admitem tais recursos, como os aplicativos de banco; e
• utilizar autenticação dupla (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.

2) Após roubo, furto, ou perda do aparelho celular:

• ligar — de imediato — para a operadora e informar o ocorrido, para bloqueio do *chip*;
• atentar para o fato de que, quanto mais tempo se deixar o *chip* habilitado, mais tempo haverá para a execução de fraude;
• registrar um boletim de ocorrência na delegacia de polícia mais próxima ou pela Internet — serão necessários os números do IMEI e de série do aparelho;
• desconectar o dispositivo das contas de *e-mail,* das redes sociais e de outros serviços (*Gmail, Facebook, Instagram, Twitter* etc); e
• programar a exclusão dos dados pelo *site* do fabricante (*Google, Apple* etc*).*

CLASSIFICADO

Segurança da Informação — Órgão de Registro Nível 1 (ORN 1)

Falamos em edições anteriores sobre o processo de habilitação e credenciamento de segurança para o tratamento de informação classificada dos órgãos e entidades da Administração Pública federal, bem como de entidades privadas que com eles mantenham vínculo.

Órgão de Registro Nível 1 (ORN1) é um ministério ou órgão de nível equivalente, habilitado pelo Núcleo de Segurança e Credenciamento para o tratamento da informação classificada.

Vamos conhecer um pouco mais sobre o que compete ao ORN1?

I - Habilitar Órgão de Registro Nível 2 (ORN2), órgão ou entidade, pública ou privada, vinculado ao ORN1, para credenciar pessoa para o tratamento de informação classificada.

II - Habilitar posto de controle de órgão ou entidade, pública ou privada, que com ele mantenha vínculo de qualquer natureza, para o armazenamento de informação classificada em qualquer grau de sigilo.

III - Credenciar pessoa que com ele mantenha vínculo de qualquer natureza, para o tratamento de informação classificada.

IV- Realizar inspeção e investigação para credenciamento de segurança, necessárias à execução do previsto no inciso III, acima.

V - Fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança para o tratamento de informação classificada, no âmbito de suas competências.

Todas as características do ORN1 são previstas no Art. 7o do Decreto no 7.845, de 14 de novembro de 2012, o qual regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Para saber mais informações sobre esse assunto ou outras informações sobre segurança da informação acesse: http://dsic.planalto.gov.br .

Cuidados no ambiente de trabalho

O cuidado de todas as pessoas no ambiente de trabalho é essencial para a Segurança da Informação nas organizações. Além dos cuidados da alta administração, que podem contemplar, entre outras ações, a implementação de uma Política de Segurança da Informação, a instalação de câmeras de segurança e de meios de controle de acesso, a atenção de todos os indivíduos é muito importante.

Como exemplo, as informações só devem ser acessadas pelas pessoas que realmente delas necessitam e que podem conhecê-las. Assim, deve-se atentar para quem as informações são encaminhadas. Deve-se, ainda, procurar utilizar, sempre que possível, armários e gavetas com chave para armazenar documentos físicos, e utilizar trituradoras para descarte dos documentos que não são públicos.

O acesso aos sistemas também merece um cuidado especial. Devem ser utilizadas senhas que combinem letras, números, e caracteres especiais, como asteriscos, por exemplo. As senhas não devem ser compartilhadas e devem ser trocadas periodicamente. Outro cuidado importante é sempre bloquear a estação de trabalho quando não estiver sendo utilizada.

Zelar pela Segurança da Informação é dever de todos!

Fonte: http://dsic.planalto.gov.br/ https://www.ctir.gov.br/
Editorial/redação/diagramação: DSI Sugestões: asscom.dsi@presidencia.gov.br