BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 07 – Agosto/2020

Como agir nos casos de perfis falsos em redes sociais

Com o crescente uso das redes sociais e a disponibilidade de diversos aplicativos voltados à comunicação, surgiram, também, atividades ilícitas que visam prejudicar os usuários. Uma delas é a criação de contas ou de perfis falsos para alcançar algum objetivo criminoso. A transmissão pode gerar consequências danosas para a imagem do servidor, para o seu cargo e para o órgão a que pertence.

É recomendado, ao verificar uma conta em que fingem ser você, apresentar imediata denúncia do fato ao aplicativo utilizado. O registro do boletim de ocorrência (BO) em delegacia de polícia é também necessário, para possíveis medidas judiciais. Lembre-se de guardar as evidências do perfil falso: fotos ou capturas de tela (*printscreen*), conversas privadas e publicações.

Para evitar cair neste golpe, sugerimos:

- nas configurações do aplicativo, ajuste os parâmetros de privacidade para impedir que estranhos acessem suas fotos e seus dados pessoais;
- não adicione pessoas desconhecidas;
- utilize *software* de segurança e senhas complexas;
- desative contas sem uso;
- iniba a função do GPS nos aplicativos e câmeras de seu aparelho; e
- tenha em mente que suas publicações *online* são permanentes - mesmo que você apague a postagem ou elimine a conta, alguém pode ter capturado a tela com suas mensagens e fotografias para utilizá-las posteriormente.

Indicamos a leitura das Recomendações nº 02/2019, nº 03/2019 e nº 04/2019, constantes em https://www.ctir.gov.br/alertas/, para realização específica da denúncia em cada rede social mais utilizada.

Internet das Coisas

A *Internet* das Coisas, também conhecida como *IoT*, abreviação do termo em inglês *"Internet of Things",* refere-se à conexão de dispositivos para troca de informações com pessoas e com outros equipamentos.

Essa nova tecnologia ampliou a possibilidade de comunicação entre diversos aparelhos. Antes restrita a computadores, celulares e *tablets*, por exemplo, está agora disponível em carros, eletrodomésticos e até em ferramentas médicas, podendo ser conectados à *Internet* ou apenas à rede doméstica.

Assim, a *Internet* das Coisas tem sido empregada em soluções para gerar conforto no cotidiano do usuário: acionar uma lâmpada ou um ar condicionado por meio do celular, usar robôs de limpeza, carros autônomos e até vigiar espaços públicos.

Com a grande conexão de equipamentos que essa tecnologia permite, surgiram os conceitos de "Casas Inteligentes" e de "Cidades Inteligentes".

Por outro lado, um grande desafio é a garantia da segurança nestes aparelhos. A privacidade e a proteção de dados merecem especial atenção, devido à coleta e à transmissão de dados de alguns dispositivos de *IoT*.

Para reduzir os riscos de ataques cibernéticos e a má utilização dos dados trafegados, devem ser observados requisitos mínimos de segurança da informação ao se optar pela utilização dessas soluções.

Em edições anteriores, falamos sobre as características do Posto de Controle (PC) e sobre o processo de credenciamento de segurança para o tratamento de informação classificada na administração pública federal (APF).

Você sabia que toda informação classificada, em qualquer grau de sigilo e quando em formato digital, deverá - obrigatoriamente - ser protegida com recurso criptográfico baseado em algoritmo de Estado?

Recurso criptográfico é um sistema, programa, processo, equipamento isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para cifrar ou decifrar informações.

Algoritmo de Estado, por sua vez, é uma função matemática, desenvolvida pelo Estado, utilizada na cifração e na decifração de informações, para uso exclusivo do serviço de órgãos ou entidades do Poder Executivo federal.

A informação classificada em grau de sigilo, em formato digital, deve ser cifrada utilizando recursos criptográficos baseados em algoritmo de Estado, em concordância com os requisitos mínimos estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

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