BIM
Boletim Informativo Mensal
Comunicar para Educar
Fevereiro/2022 – Ano 3 – nº 25

Golpes nas Redes Sociais!

Uma peça essencial na execução dos crimes cibernéticos é a **Engenharia Social**. Trata-se de técnica utilizada por criminosos virtuais para persuadir e manipular pessoas, a fim de obter informação privilegiada. Por meio dessa técnica, a vítima pode ser induzida a revelar dados confidenciais, infectar seu computador com *malware* ou abrir *links* que direcionam para sites maliciosos.

As **redes sociais** são solo fértil para coleta de informações pessoais e, por isso, são muito visadas por golpistas, que normalmente buscam obter dados, credenciais, nome de usuário e senha de acesso destes aplicativos, para o cometimento de crimes.

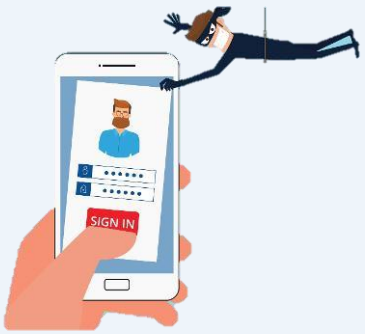
Exemplos de crimes utilizando técnicas de Engenharia Social:

1) por meio do *WhatsApp*

O enganador convence a vítima (por telefone, *e-mail*, mensagem de texto) a escanear um **QR *code***, que se encontra em uma **página falsa**, e sequestra a sessão de WhatsApp, assumindo o controle do aplicativo.

Como evitar?

- Desconfie de anúncio que peça para escanear QR *code* em troca de algum benefício.
- Mantenha o antivírus sempre atualizado em todos os seus dispositivos conectados à *internet* (celular, *tablet* e *notebook*).
- Evite o uso de redes de *internet wi-fi* públicas, particularmente, em aeroportos e restaurantes.



2) por meio do *Instagram*

- O golpista cria um **perfil falso** utilizando o **nome de uma vítima** que efetivamente tem uma conta pública no Instagram. O perfil falso vai reproduzir as fotos e os posts feitos pela vítima, duplicando conteúdos, por meio de *prints* da tela e de cópia dos textos nas legendas;
- Depois começa a seguir os mesmos amigos e posta mensagens públicas, onde se identifica como vítima de um golpe e explica o transtorno provocado pelo suposto ataque *hacker*, argumentando que perdeu o acesso às contas de mídias sociais e aos aplicativos de banco;
- O passo seguinte é enviar uma mensagem direta para os contatos que manifestaram pesar ou solidariedade com a situação. Na mensagem, o criminoso pede um valor baixo que deverá ser transferido para uma carteira virtual. **A promessa é devolver o valor assim que possível**;
- O valor é direcionado para a carteira virtual do golpista, ou de um " laranja". Neste caso, não ocorreu nenhum ataque hacker, e sim o **estelionato.**

Como evitar?

- Utilize a autenticação de dois fatores.
- Ative a "solicitação de *login*".
- Divulgue para sua comunidade ser necessário estar atenta a perfis suspeitos e denunciá-los .
- Jamais forneça dados pessoais para perfis desconhecidos.
- Desconfie quando esses dados forem solicitados por meio de mídias sociais.

Na última década, a incidência do uso de redes sociais pelos cidadãos brasileiros aumentou consideravelmente, e, nesse contingente humano, incluem-se os **servidores públicos**. Os golpes se tornaram tão frequentes, que, em 2018, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, CTIR Gov/DSI/GSI, emitiu recomendações sobre como os golpes cometidos nas redes sociais são aplicados e como evitá-los (Alerta Nº 2/2018).

BIM
Boletim Informativo Mensal
Comunicar para Educar
Fevereiro/2022 – Ano 3 – nº 25

Publicada Nova Instrução Normativa do GSI

Com o objetivo de orientar os integrantes dos órgãos e das entidades da administração pública federal, sobre o uso seguro de mídias sociais, no que se refere aos perfis institucionais, publicou-se a Instrução Normativa (IN) nº 6, de 23 de dezembro de 2021, do Gabinete de Segurança Institucional da Presidência da República.

A IN nº 6, de 2021, conforme seu artigo 1º, estabelece requisitos mínimos para o uso seguro de mídias sociais pelos órgãos e pelas entidades do Poder Executivo federal para que administrem seus perfis institucionais com segurança e confiabilidade no atendimento à sociedade.

A publicação da nova norma faz parte do processo de revisão e de consolidação dos atos normativos inferiores a decreto editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional, que vem ocorrendo no GSI desde 2020, conforme determinado pelo Decreto nº 10.139, de 28 de novembro de 2019.

No presente caso, a IN nº 6, de 2021, substitui a Norma Complementar nº 15, de 2012, do GSI, visando à atualização das disposições sobre o assunto, o que teve como base consulta a todos os órgãos do Poder Executivo federal listados no art. 9º do Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação (PNSI).

Sendo assim, essa IN pretende contribuir para assegurar:

- a disponibilidade das informações — para evitar que o conteúdo do perfil institucional se torne indisponível aos usuários;
- a integridade das informações — para prevenir que as informações disponíveis no perfil institucional sejam alteradas de forma indevida;
- a confidencialidade das informações — para impedir que haja publicação de informações confidenciais no perfil institucional e, em especial, a divulgação indevida de dados pessoais; e
- a autenticidade das informações — para garantir que quem acessa o perfil institucional seja quem diz ser e possua a devida autorização para o acesso.

Informação classificada como ULTRASSECRETA

Na edição anterior falamos da Informação Classificada no grau de sigilo SECRETO. Agora falaremos da informação classificada no grau ULTRASSECRETO.

Uma informação pode ser classificada como ULTRASSECRETA, quando for considerada imprescindível à segurança da sociedade ou do Estado, levando em conta o risco ou o dano á segurança e o prazo, sendo essa a classificação de mais alto nível.

Os processos de expedição, condução e entrega de documento com informação classificada como ULTRASSECRETA devem ser feitos pessoalmente por agente público autorizado, ou transmitidas por meio eletrônico com uso de recurso criptográfico.

O prazo máximo de classificação da informação classificada como ULTRASSECRETA é de até 25 anos, que é contado a partir de sua produção. As autoridades que possuem competência para classificar nesse grau são: o Presidente da República; o Vice-Presidente da República; os Ministros de Estado (e autoridades com as mesmas prerrogativas); os Comandantes das Forças Armadas; e os Chefes de Missões Diplomáticas e Consulares permanentes no exterior.

Os agentes públicos que classificam a informação no grau ULTRASSECRETO também têm competência para classificar as informações nos graus SECRETO e RESERVADO.

Para saber mais sobre esse assunto acesse link: https://www.gov.br/gsi/pt-br/centrais-de-conteudo/publicacoes/legislacao/Lei_10683

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br