BIM
Boletim Informativo Mensal
Comunicar para Educar
Outubro/2023 - Ano 4 - nº 42

Cuidado com *Links* Maliciosos em Redes Sociais

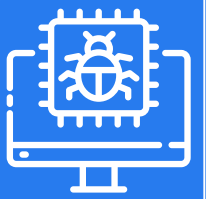
Uma ameaça séria e cada vez mais presente nas redes sociais é o recebimento de *links* maliciosos que visam cometer fraudes bancárias. Golpistas estão cada vez mais sofisticados, criando mensagens e postagens persuasivas para induzir os usuários a clicarem nesses *links* e, assim, comprometer sua segurança. Portanto, fique atento!

O que são *links* maliciosos? São URLs disfarçados que aparentam ser confiáveis, mas, na realidade, levam a páginas falsas ou infectadas por *malware*. Os golpistas estão cada vez mais sofisticados, criando mensagens criativas e contextualizadas para induzir os usuários a clicarem nesses *links* e, assim, comprometer sua segurança ou obter vantagens financeiras ilícitas.

Neste contexto, temos observado uma prática fraudulenta envolvendo o programa governamental "Desenrola Brasil" nas plataformas *WhatsApp*, *Facebook* e *Instagram*. É crucial estar ciente desses riscos e tomar medidas preventivas para salvaguardar suas informações financeiras e pessoais. Uma vez que você clicar em um *link* malicioso, estará sujeito a diversas ameaças, incluindo:

***Phishing*: *sites* fraudulentos que se passam por páginas legítimas de bancos ou instituições financeiras, com o objetivo de obter suas informações confidenciais, como senhas e números de cartões, ou desvio de dinheiro;**

Roubo de Identidade: os criminosos podem usar as informações obtidas para se passar por você, contrair empréstimos ou realizar compras fraudulentas em seu nome;



Instalação de *Malware*: alguns *links* podem infectar seu dispositivo com *malware*, permitindo que *hackers* acessem seus dados ou monitorem suas atividades; e

***Ransomware*: alguns *links* levam a *downloads* de *ransomware*, que bloqueiam o acesso ao seu dispositivo e exigem pagamento para liberá-lo.**

Para proteger-se contra essas ameaças, siga as seguintes medidas:

Desconfie de *links* não solicitados: não clique em *links* enviados por estranhos ou que pareçam suspeitos, mesmo que sejam compartilhados por conhecidos;

Busque sempre os canais oficiais das instituições financeiras para buscar informações sobre negociações;

Verifique a URL: antes de clicar em um *link*, passe o cursor sobre ele para verificar se o endereço corresponde ao *site* oficial do banco ou empresa mencionada;

Evite fornecer informações pessoais: bancos e instituições financeiras nunca pedem informações confidenciais por meio de mensagens em redes sociais;

Mantenha seu dispositivo atualizado: mantenha seu sistema operacional, navegadores e aplicativos de segurança sempre atualizados para se proteger contra vulnerabilidades conhecidas;

Use autenticação de dois fatores: ative a autenticação de dois fatores em suas contas bancárias para adicionar uma camada extra de segurança;

Utilize uma VPN: uma VPN (rede virtual privada) protege sua conexão e mantém suas informações mais seguras ao utilizar redes públicas.

A segurança de suas informações pessoais e financeiras é uma responsabilidade compartilhada entre você e as instituições financeiras. Ao detectar qualquer atividade suspeita ou se você acredita ter sido vítima de uma fraude, entre em contato imediatamente com o seu banco e reporte o incidente.

Cartilha de Gestão de Segurança da Informação

A Cartilha de Gestão de Segurança da Informação foi elaborada por demanda do Comitê Gestor de Segurança da Informação (CGSI), que assessora o GSI/PR quanto às atividades relacionadas à segurança da informação, com os objetivos de:

- orientar os gestores de segurança da informação no desempenho de suas atribuições e competências;
- esclarecer as responsabilidades dos envolvidos no processo de segurança da informação; e
- apresentar a estrutura de segurança da informação aplicável dos órgãos e entidades da administração pública federal, os normativos aplicáveis, o vocabulário utilizado, dentre outras informações relevantes.

Ela está dividida em três capítulos: Segurança da Informação; Responsabilidades; e Boas práticas em segurança da informação.

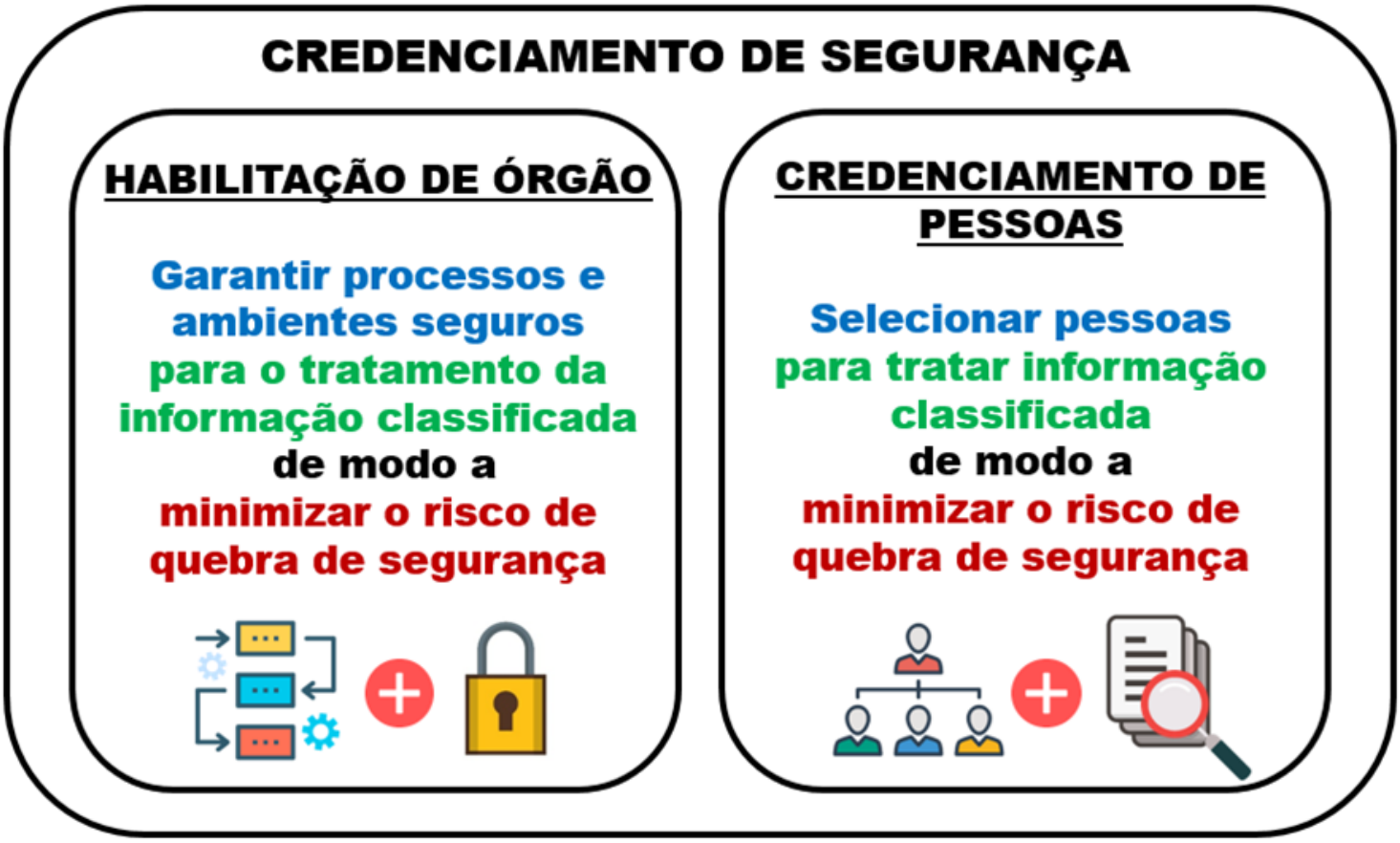
Fiquem à vontade para ler e compartilhar esse material, que está disponível em formato pdf no *site* do DSIC (https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/cartilha-de-gestao-de-seguranca-da-informacao/CartilhadeSegurancaInformao.pdf).

Credenciamento de Segurança

O ato de credenciar significa atribuir licença ou poderes que permitam a representação oficial em nome de alguém ou de alguma instituição ou, ainda, conceder habilitação para o desempenho de determinada atividade ou função.

A ação descrita acima é muito comum em nosso dia a dia. Ela pode ser observada, por exemplo, no simples cadastro pessoal que permite a entrada em edifícios públicos ou comerciais e na terceirização da prestação de serviço por agente ou empresa credenciada.

Sobre o assunto, é importante o conhecimento da existência do Credenciamento de Segurança, tipo especial de credenciamento pouco conhecido por ser menos comum no cotidiano da população, cujo objetivo é habilitar órgão ou entidade e credenciar pessoa para o tratamento de informação classificada como RESERVADA, SECRETA ou ULTRASSECRETA.



Por fim, vale destacar que o Núcleo de Segurança e Credenciamento foi instituído pela Lei de Acesso à Informação no âmbito do Gabinete de Segurança Institucional da Presidência da República para, dentre outras finalidades, promover e propor a regulamentação do Credenciamento de Segurança.

Para saber mais sobre este assunto e outros relacionados à segurança da informação acesse: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic.

Fonte: https://www.gov.br/gsi/dsic/
Editorial/redação/diagramação: SSIC Sugestões: educa.si@presidencia.gov.br