Comunicar para Educar
Março/2023 - Ano 4 - nº 37

BIM

Boletim Informativo Mensal

Instrução Normativa, aliada na resiliência cibernética!

As Instruções Normativas (IN), emitidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), estabelecem diretrizes e procedimentos para elevar os níveis de segurança dos ativos de informação, além de prevenir a ocorrência de incidentes cibernéticos, portanto trata-se de normas essenciais para consulta de todo profissional do governo federal envolvido com segurança da informação e cibernética. Além disso, serve de referência para os profissionais dos demais setores da sociedade.

Vale ressaltar que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II.

Entenda quais são e como se proteger dos principais golpes do Pix.

1) Golpe do falso funcionário do banco

O criminoso se passa por funcionário de uma instituição financeira, entra em contato com a vítima, por telefone ou mensagem de texto, e pede para que ela faça uma transferência, por meio do Pix, para proteger sua conta bancária ou para receber algum tipo de recompensa.

2) Golpe do QR Code

O criminoso substitui o código verdadeiro, disponibilizado na loja ou no estabelecimento comercial, por um QR Code falso. Quando a vítima escaneia o código falso e realiza a transferência, via Pix, o dinheiro vai para a conta do golpista.

3) Golpe da troca de chave Pix

Nesse golpe, o criminoso se aproveita da falta de conhecimento da vítima sobre o funcionamento do sistema e pede para que ela troque a chave Pix cadastrada em sua conta por uma chave falsa. Com isso, os valores transferidos nas transações Pix da vítima são direcionadas para a conta dos golpistas.

4) Golpe da clonagem de celular

O criminoso clona o celular da vítima e acessa sua conta bancária para fazer transferências via Pix. Para isso, ele geralmente utiliza informações obtidas por meio de engenharia social, como senhas e códigos de segurança.

5) *Malware* do tipo "Pix"

Golpe que tem se popularizado no Brasil recentemente, onde criminosos enviam mensagens falsas para as vítimas solicitando que se atualize um aplicativo ou *click* em um *link*. Ao realizar a ação, o *malware* é instalado no dispositivo e compromete as transações por Pix.

6) Golpe do site falso

Envio de *links* por meio de aplicativos de mensagens ou *e-mail*, onde os criminosos se fazem passar por instituições financeiras, lojas ou empresas conhecidas para ganhar a confiança das vítimas. Ao clicar no *link*, a vítima é direcionada a uma página falsa que se parece com a de um banco ou empresa, onde é solicitada a realização da transferência Pix.

Como se proteger?

1) sempre verifique cuidadosamente as informações do destinatário antes de realizar a transferência, veja se os dados (nome, CPF ou CNPJ) correspondem ao destinatário correto;

2) nunca compartilhe informações confidenciais, como senhas ou códigos de segurança, com terceiros. Os golpistas geralmente tentam obter essas informações por meio de engenharia social, fazendo-se passar por funcionários de bancos ou de outras empresas;

3) fique atento a mensagens suspeitas, oferecendo prêmios ou promoções em troca de transferências de dinheiro via Pix. Essas mensagens, geralmente, são enviadas por meio de aplicativos de mensagens, e podem parecer muito convincentes. Confirme sempre se a mensagem é verdadeira antes de tomar qualquer ação;

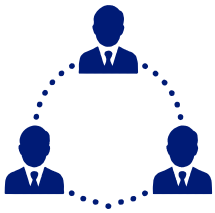
4) mantenha o seu aplicativo da instituição financeira sempre atualizado e utilize ferramentas de segurança, como autenticação em duas etapas, para evitar o acesso não autorizado à sua conta;

5) Antes de realizar qualquer transação em um *site*, verifique se ele é legítimo e seguro, e se possui um certificado de segurança; e

6) Utilize *softwares* de segurança, como antivírus e *firewalls*, para proteger seu computador ou dispositivos móveis contra *malwares* e outros tipos de ameaças.

Lembre-se que a segurança das suas informações pessoais e financeiras é fundamental. Se você perceber qualquer atividade suspeita em sua conta, entre em contato imediatamente com a sua instituição financeira para obter ajuda. A prevenção é a melhor forma de se proteger contra fraudes.

VOCÊ SABIA?



Existe um Comitê Gestor de Segurança da Informação (CGSI), no âmbito federal, composto por representantes dos órgãos da Presidência da República, de Ministérios, do Banco Central do Brasil (BACEN), da Controladoria-Geral da União (CGU), da Advocacia-Geral da União (AGU) e da Autoridade Nacional de Proteção de Dados (ANPD) com a atribuição assessorar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nas atividades relacionadas à Segurança da Informação.

O CGSI foi instituído pelo Decreto nº 9.637, de 26 de dezembro de 2018, com o objetivo de alinhar posicionamentos de alto nível e de deliberar sobre normas editadas pelo GSI/PR e ações de Governo, que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade de ativos de informação em âmbito nacional nos órgãos e entidades da administração pública federal.

Nesse sentido, o GSI/PR atualizará brevemente o art. 9º do Decreto 9.637, de 2018, para incluir no CGSI os novos órgãos e denominações que constam na organização básica dos órgãos da Presidência da República e dos Ministérios estabelecida pela Medida Provisória nº 1.154, de 1º de janeiro de 2023.

Para compreender um pouco mais sobre esse comitê, acesse seu regimento interno em:

https://www.in.gov.br/en/web/dou/-/resolucao-n-1-de11-de-setembro-de-2019-217042776.

Previna-se de Golpes Digitais do Tipo *Job Scam*

O *Job Scam* consiste em ofertas de trabalho falsas, divulgadas em diversos canais, como redes sociais, *sites* de emprego e até mesmo por *e-mail*, onde os golpistas se passam por empresas legítimas e oferecem vagas que aparentam ser muito atraentes, mas, na verdade, são armadilhas para roubar informações pessoais e financeiras.

Para evitar cair em um golpe digital como este, é importante seguir algumas recomendações básicas:

- pesquise a empresa que está oferecendo a vaga, verifique se ela é real e se tem uma boa reputação no mercado;
- não envie informações pessoais, nem realize pagamentos sem ter certeza de que trata-se de uma empresa legítima;

- desconfie de ofertas de trabalho que parecem boas demais para ser verdade, com salários muito acima do mercado ou benefícios muito generosos. Nesses casos, é preciso investigar a fundo para evitar cair em uma armadilha;

- tenha cuidado com *links* suspeitos e arquivos anexos em *e-mails* que, supostamente, são de empresas de recrutamento;
- crie um *e-mail* especifico para o cadastro em sites de emprego; e
- evite anexar fotos e informar dados bancários.

Em resumo, a segurança da informação e cibernética é um assunto que precisa estar presente no dia a dia de todos os usuários da *internet*, especialmente quando se trata de ofertas de trabalho. Com atenção e cuidado, é possível evitar cair em um *Job Scam* e proteger seus dados pessoais e financeiros. Fique atento e não se deixe enganar!

Dicas e recomendações

- Manter seus dispositivos atualizados com as versões mais recentes dos sistemas operacionais e aplicativos é importantíssimo para garantir a segurança da informação e cibernética. As atualizações, geralmente, incluem correções de segurança importantes que podem evitar que ameaças explorem vulnerabilidades conhecidas. Além disso, as atualizações também podem melhorar o desempenho do dispositivo e adicionar novos recursos.

- Trate suas senhas com máximo cuidado e busque seguir as orientações abaixo:
  não compartilhe sua senha — ela é somente sua, e deve ser de uso pessoal e intransferível;
  não deixe suas senhas escritas em local de fácil acesso, para evitar seu uso indevido por terceiros; e
  crie senhas fortes, elas são mais difíceis de ser quebradas, por tentativas não autorizadas — use caracteres especiais (Ex.: *, &, $, #), e evite algo óbvio, semelhante a “123senha”

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