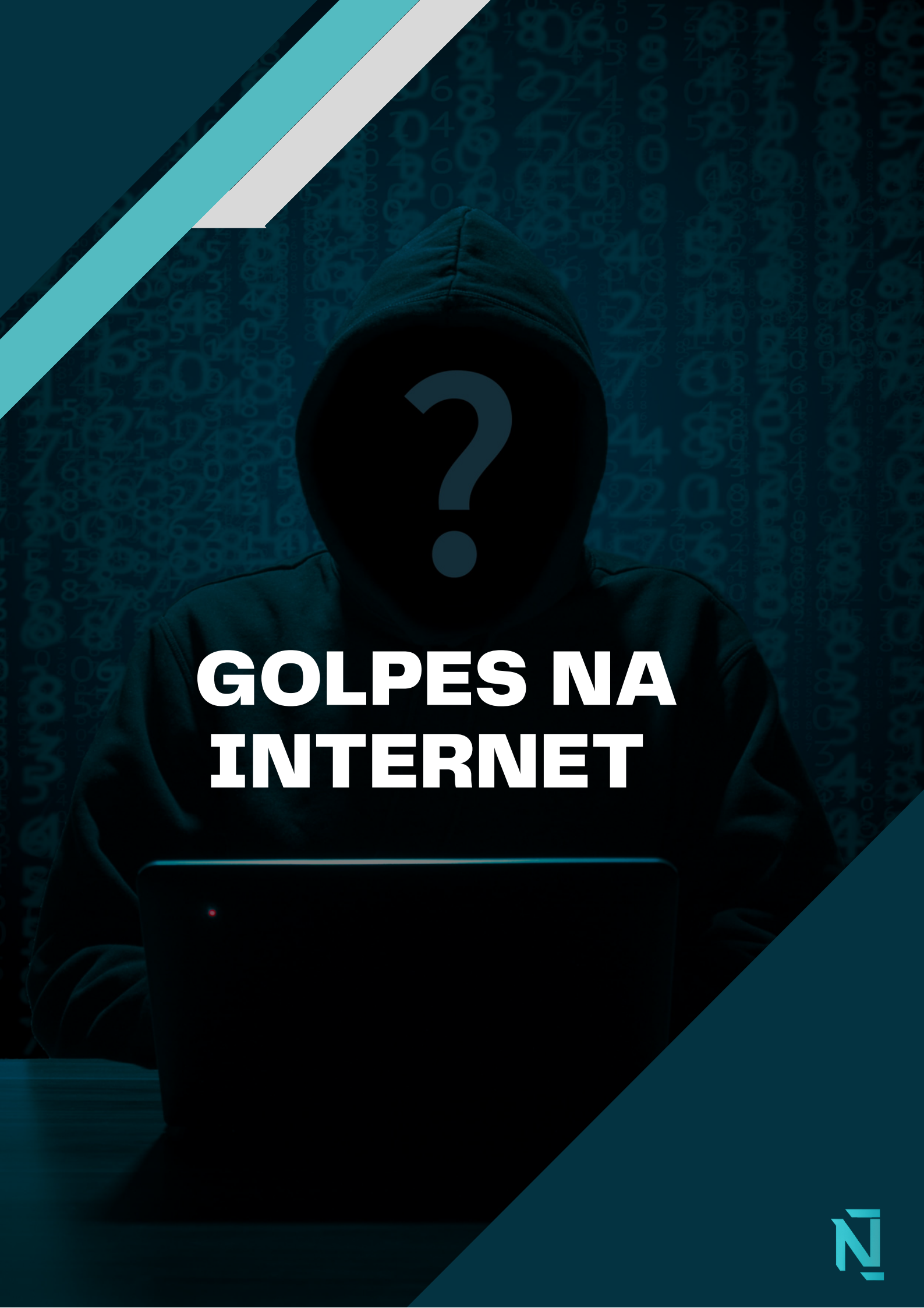

GOLPES NA INTERNET

GOLPES NA INTERNET

Recife 2023

Bem-vindos à cartilha de segurança da internet NICS! Em um mundo cada vez mais conectado, onde a internet desempenha um papel fundamental em nossa vida cotidiana, é crucial estarmos bem informados sobre como navegar de maneira segura e protegida no vasto mundo virtual. A marca NICS tem o prazer de apresentar a você esta cartilha abrangente, repleta de orientações práticas e dicas essenciais para garantir que sua experiência online seja não apenas enriquecedora, mas também segura.

A segurança na internet é uma questão que afeta a todos, desde indivíduos até empresas. O uso crescente de dispositivos digitais para comunicação, transações financeiras, compras online e acesso a informações importantes requer uma conscientização profunda sobre os possíveis riscos e ameaças que podem surgir ao longo do caminho. É nesse contexto que a NICS surge como uma aliada confiável, dedicada a fornecer conhecimento e ferramentas para capacitar você a tomar decisões informadas e proteger sua presença digital.

Ao longo desta cartilha, exploraremos uma variedade de tópicos cruciais relacionados à segurança da internet. Desde a criação de senhas robustas até a identificação de e-mails de phishing, passando pela importância da atualização de software e pela proteção da privacidade online, nossa missão é equipar você com as habilidades necessárias para se movimentar com confiança em um ambiente virtual muitas vezes complexo e em constante evolução.

Acreditamos que a segurança na internet é um direito fundamental de todos os usuários, independentemente de sua idade, experiência ou nível de conhecimento técnico. Portanto, convidamos você a embarcar nesta jornada conosco, explorando os diversos capítulos que preparamos para ajudar você a se tornar um participante consciente e responsável no mundo digital. Lembre-se, sua segurança é nossa prioridade, e a cartilha NICS é o seu guia confiável para uma experiência online mais segura e protegida. Vamos começar essa jornada juntos!

EXPLORAÇÃO CIBERNÉTICA: GOLPES ONLINE E MEDIDAS DE PROTEÇÃO

Geralmente, não é uma tarefa fácil invadir e manipular informações em um servidor de uma entidade bancária ou comercial, e por essa razão, indivíduos fraudulentos estão concentrando seus esforços em explorar as fraquezas dos usuários. Através do uso de métodos de manipulação social e por meio de diferentes abordagens, os golpistas buscam ludibriar e convencer as possíveis vítimas a compartilhar dados sensíveis ou a realizar ações, como executar códigos prejudiciais e acessar páginas falsas.

Ao obter os detalhes das vítimas, os trapaceiros frequentemente conduzem transações financeiras, entram em sites, enviam mensagens eletrônicas, estabelecem empresas fictícias e criam contas bancárias ilegítimas, juntamente com outras atividades de má-fé.

Vários dos esquemas perpetrados na Internet têm potencial para serem considerados delitos contra o patrimônio, enquadrando-se como formas de estelionato. Desta maneira, o indivíduo enganador pode ser categorizado como um estelionatário.

Nas próximas seções, serão apresentados alguns dos principais estratagemas empregados online, bem como algumas precauções que você deve adotar para se resguardar contra eles.

PROTEGENDO-SE CONTRA O ROUBO DE IDENTIDADE E SUAS CONSEQUÊNCIAS

O ato de identity theft, ou seja, o roubo de identidade, envolve uma pessoa tentando se passar por outra, assumindo uma identidade falsa, com o intuito de obter vantagens não merecidas. Algumas situações de roubo de identidade podem ser consideradas como violações da ordem pública, enquadrando-se como falsificação de identidade.

No cotidiano, sua identidade pode ser comprometida caso alguém utilize seus documentos para abrir uma empresa ou uma conta bancária em seu nome. Na esfera virtual, isso também pode ocorrer quando alguém cria um perfil falso em uma rede social usando seu nome, acessa sua conta de e-mail e envia mensagens em seu nome, ou falsifica campos de e-mail para parecer que a mensagem foi enviada por você.

Quanto mais informações você compartilha sobre sua vida e rotina, mais vulnerável fica a um golpista que deseja roubar sua identidade, pois ele terá mais dados à disposição para parecer convincente. Além disso, o golpista pode empregar outras táticas e ataques para coletar informações a seu respeito, incluindo suas senhas, por meio de códigos maliciosos (consulte o capítulo sobre Malware), ataques de força bruta e interceptação de tráfego (veja o capítulo sobre Ataques na Internet).

Se sua identidade for roubada, você pode enfrentar consequências como perdas financeiras, danos à sua reputação e problemas de crédito. Além disso, reverter todos os problemas causados pelo impostor pode levar muito tempo e ser emocionalmente desgastante.

Prevenção:

A maneira mais eficaz de evitar o roubo de identidade é impedir que impostores acessem seus dados e contas de usuário (consulte o capítulo sobre Privacidade). Além disso, para evitar que suas senhas sejam obtidas e usadas indevidamente, é crucial que você seja cuidadoso ao usá-las e ao criá-las (veja o capítulo sobre Contas e Senhas).

Também é importante ficar atento a alguns sinais que podem indicar o uso indevido de sua identidade por golpistas, tais como:

- Problemas com agências de proteção de crédito que você não iniciou.

- Recebimento de e-mails que você não enviou.

- Notificações de acesso mostrando atividade em sua conta de e-mail ou perfil de rede social em momentos ou lugares em que você não estava acessando.

- Transações não autorizadas em seus extratos bancários ou cartão de crédito.

- Ligações telefônicas, correspondências e e-mails referentes a assuntos desconhecidos para você, como uma conta bancária não sua ou uma compra que você não fez.

DESMASCARANDO A FRAUDE DE ANTECIPAÇÃO DE RECURSOS: TÁTICAS E CUIDADOS

A estratégia conhecida como fraude de antecipação de recursos, ou também chamada advance fee fraud, envolve uma artimanha em que um fraudador busca convencer uma pessoa a fornecer informações confidenciais ou efetuar um pagamento adiantado, baseado na promessa de obter benefícios futuros.

Através de mensagens eletrônicas enganosas ou por meio do acesso a sites fraudulentos, a vítima é envolvida em uma situação fictícia ou uma narrativa elaborada, que justifica a necessidade de compartilhar dados pessoais ou realizar um pagamento adiantado para a suposta obtenção de vantagens futuras. Posteriormente, a vítima percebe que o benefício prometido é inexistente, revelando-se vítima de uma fraude e tendo seus dados ou dinheiro sob posse dos golpistas.

Um exemplo notório desse tipo de fraude é o "Golpe da Nigéria", também conhecido como Nigerian 4-1-9 Scam, que geralmente segue este padrão:

a. A vítima recebe um e-mail em nome de alguém ou de uma suposta instituição da Nigéria, solicitando que ela atue como intermediária em uma transferência internacional de fundos.

b. O valor mencionado na mensagem é extremamente alto e, caso a vítima aceite intermediar a transação, promete-se uma porcentagem desse valor como recompensa futura.

c. A razão para a seleção da vítima geralmente é atribuída a uma indicação por um conhecido ou suposto funcionário, destacando sua honestidade e confiabilidade.

d. O e-mail enfatiza a ilegalidade da transferência e pede absoluto sigilo e resposta urgente, alertando que perder a oportunidade implicaria na busca por outro parceiro.

e. Após aceitar a proposta, os golpistas solicitam que a vítima pague antecipadamente uma quantia significativa (porém inferior ao valor prometido) para cobrir custos como honorários advocatícios e taxas de transferência.

f. Após realizar o pagamento solicitado, a vítima é informada de novas despesas ou perde o contato com os fraudadores.

g. Eventualmente, a vítima percebe que, além de perder o dinheiro investido, nunca receberá a recompensa prometida e seus dados podem estar sendo indevidamente utilizados.

Embora esse golpe seja conhecido como originário da Nigéria, casos semelhantes têm sido registrados envolvendo outros países, frequentemente provenientes de regiões empobrecidas ou em meio a conflitos políticos, econômicos ou raciais.

A fraude de antecipação de recursos apresenta múltiplas variações que, apesar de possuírem discursos distintos, compartilham características semelhantes em sua aplicação e nos prejuízos causados. Algumas dessas variações incluem:

Existem diversas formas de golpes online, cada um com seu próprio disfarce e artimanhas para enganar pessoas incautas. Aqui estão alguns exemplos comuns:

Loteria Internacional: Você recebe um e-mail alegando que ganhou em uma loteria internacional, porém, para receber seu prêmio, precisa compartilhar dados pessoais e informações bancárias.

Oferta de Crédito Fácil: Chega um e-mail oferecendo empréstimos ou financiamentos com taxas de juros muito abaixo das normais. Após a aprovação fictícia, é solicitado um depósito para "cobrir despesas".

Doação de Animais: Ao buscar por animais de raça, você encontra anúncios de doação. Depois de entrar em contato, pedem dinheiro para "custos de transporte".

Proposta de Emprego: Um SMS promete uma oferta de emprego atraente, mas para seguir adiante, precisa fornecer detalhes de sua conta bancária.

Noiva Russa: Mensagens insinuam um relacionamento internacional e pedem ajuda financeira para viagens.

A melhor maneira de se proteger é saber identificar os sinais de tentativas de golpe. Essas mensagens geralmente exibem características como:

- Promessas de dinheiro exageradamente altas.
- Pedidos de sigilo.
- Pressão por uma resposta rápida.
- Uso de palavras como "urgente" e "confidencial" no assunto.
- Erros gramaticais e ortográficos (gerados por tradutores automáticos).

Além disso, adotar uma postura cautelosa pode prevenir muitos golpes. Portanto, considere:

- Questionar por que você foi escolhido para a oferta.
- Desconfiar de situações em que deve pagar antecipadamente para receber um valor maior no futuro.

Lembre-se dos ditados populares como "Quando a esmola é demais, o santo desconfia" e "Tudo que vem fácil, vai fácil". Esses princípios podem te orientar nessas situações.

Importante ressaltar que nunca se deve responder a essas mensagens, pois isso pode validar seu endereço de e-mail, o que pode levar a mais spam ou outros tipos de golpes. Mantenha-se vigilante e alerta para não cair nessas ciladas virtuais.

PHISHING

Phishing, também conhecido como phishing-scam ou phishing/scam, é um tipo de fraude que combina táticas técnicas e manipulação psicológica, em que um golpista tenta adquirir informações pessoais e financeiras de um usuário.
Esse ardil acontece por meio do envio de e-mails que:

- Fingem ser comunicações oficiais de instituições conhecidas, como bancos, empresas ou sites populares.

- Buscam atrair o usuário com curiosidade, promessas de caridade ou oportunidades financeiras.

- Alertam sobre consequências sérias se procedimentos não forem seguidos, como inscrição em serviços de proteção de crédito ou cancelamento de contas.

- Incitam o usuário a fornecer dados confidenciais e financeiros através de páginas falsas, tentando se passar por sites legítimos, ou por meio de códigos maliciosos projetados para coletar informações sensíveis, ou ainda por meio de formulários dentro da mensagem ou em páginas web.

As mensagens de phishing abordam uma variedade de tópicos e temas, muitas vezes explorando anúncios, serviços, personalidades e tópicos em destaque no momento.

Situações comuns que envolvem phishing incluem:

- Páginas falsas de comércio eletrônico ou internet banking: Um e-mail, em nome de um site de comércio eletrônico ou instituição financeira, tenta convencer você a clicar em um link que o leva para uma página falsa, similar ao site que você deseja acessar, onde são solicitados seus dados pessoais e financeiros.

- Páginas falsas de redes sociais ou companhias aéreas: Mensagens contendo links para o site de sua rede social ou companhia aérea. Ao clicar, você é levado a uma página falsa onde lhe pedem suas credenciais, que podem ser usadas por golpistas para acessar sua conta e realizar ações em seu nome.

- Mensagens com formulários: Você recebe um e-mail contendo um formulário para digitar informações pessoais e financeiras. A mensagem solicita que você preencha e confirme o envio, transmitindo seus dados para os golpistas.

- Mensagens com links para códigos maliciosos: Um e-mail que tenta persuadi-lo a clicar em um link para baixar e abrir/executar um arquivo. Ao fazer isso, um código malicioso é instalado em seu computador.

A melhor defesa contra o phishing é a conscientização e a capacidade de identificar sinais de tentativas de golpes. Mantenha-se atento a mensagens suspeitas e evite fornecer informações confidenciais ou clicar em links duvidosos. Desconfie de pedidos urgentes, erros gramaticais e de mensagens que prometem recompensas excepcionais. Lembre-se: proteger seus dados é um passo fundamental para navegar com segurança online.

PHARMING E GOLPES DE COMÉRCIO ELETRÔNICO: PROTEJA-SE CONTRA ATAQUES ONLINE

O termo "pharming" refere-se a um tipo específico de ataque phishing que envolve a manipulação do serviço de DNS (Domain Name System) para redirecionar a navegação do usuário para sites falsos. Nesse cenário, quando você tenta acessar um site legítimo, seu navegador é redirecionado automaticamente para uma página falsa. Isso pode ocorrer por:

- Comprometimento do servidor de DNS do provedor utilizado.

- Ação de códigos maliciosos que alteram o comportamento do serviço de DNS do seu computador.

- Ataque direto de um invasor que tenha acesso às configurações do serviço de DNS do seu computador ou modem de banda larga.

Prevenção:

- Fique alerta se, ao digitar uma URL, você for redirecionado para outro site que tenta realizar ações suspeitas, como abrir um arquivo ou instalar um programa.

- Desconfie imediatamente se o site de comércio eletrônico ou internet banking que você está acessando não utiliza uma conexão segura. Sites confiáveis sempre usam conexões seguras para solicitar dados pessoais e financeiros.

- Verifique se o certificado apresentado pelo site corresponde ao do site verdadeiro.

*

Golpes de Comércio Eletrônico

Golpes de comércio eletrônico ocorrem quando golpistas exploram a relação de confiança entre as partes em uma transação comercial para obter vantagens financeiras. Um exemplo é o golpe do site de comércio eletrônico fraudulento, no qual o golpista cria um site falso para enganar os clientes e não entrega os produtos após o pagamento.

Para aumentar o sucesso desse golpe, o golpista utiliza táticas como spam, publicidade em links patrocinados, descontos falsos em sites de compras coletivas e oferta de produtos populares a preços muito abaixo do mercado.

Além dos compradores prejudicados, outras vítimas podem incluir empresas cujo nome é associado ao golpe, sites de compras coletivas que intermediaram a transação e pessoas cujas identidades foram usadas para criar o site falso ou abrir empresas fictícias.

Prevenção:

- Pesquise o mercado e compare os preços do produto no site com os valores encontrados. Desconfie de preços muito abaixo do praticado pelo mercado.

- Antes de efetuar uma compra, pesquise na Internet sobre o site para ver as opiniões de outros clientes.

- Acesse sites especializados em lidar com reclamações de consumidores insatisfeitos para verificar se existem queixas relacionadas a essa empresa.

- Esteja atento a propagandas recebidas por meio de spam.

- Seja cauteloso ao clicar em links patrocinados.

- Verifique os dados de cadastro da empresa no site da Receita Federal para validação.

- Evite fornecer dados de pagamento caso o site não ofereça conexão segura ou não apresente um certificado confiável.

DESINFORMAÇÃO (HOAX)

A desinformação, também conhecida como hoax, refere-se a mensagens que contêm conteúdo falso ou alarmante e geralmente têm como fonte ou autora alguma instituição, empresa significativa ou órgão governamental. Ao analisar com atenção o conteúdo dessas mensagens, muitas vezes é possível identificar informações inconsistentes e tentativas de golpes, como correntes e esquemas de pirâmide.

A disseminação de desinformação pode acarretar diversos problemas, tanto para aqueles que as recebem e as compartilham, quanto para aqueles mencionados em seus conteúdos. Entre os problemas associados a desinformação estão:

- Inclusão de códigos maliciosos;

- Propagação de informações incorretas na internet;

- Ocupação desnecessária de espaço nas caixas de entrada de e-mails dos usuários;

- Comprometimento da credibilidade e reputação de pessoas ou entidades citadas na mensagem;

- Comprometimento da credibilidade e reputação de quem compartilha, pois ao fazer isso, a pessoa supostamente endossa ou concorda com o conteúdo da mensagem;

- Aumento excessivo na carga de servidores de e-mail e no consumo de largura de banda de rede, devido à transmissão e processamento das mensagens;

- Sugestão de ações a serem tomadas que, se seguidas, podem resultar em sérios danos, como a exclusão de um arquivo que supostamente contém um código malicioso, quando, na realidade, é uma parte vital do sistema operacional do computador.

Para prevenir a disseminação de desinformação, é importante verificar a origem dos e-mails e, mesmo que o remetente seja familiar, assegurar-se de que o conteúdo não seja uma desinformação. Geralmente, uma desinformação apresenta pelo menos uma das seguintes características:

- Afirma que não é uma desinformação;

- Sugere consequências trágicas se uma tarefa específica não for realizada;

- Promete ganhos financeiros ou prêmios mediante uma ação específica;

- Contém erros gramaticais e ortográficos;

- Apresenta informações contraditórias.

Claro, aqui estão as informações com os links dos sites mencionados:

Realce da Urgência: Muitas vezes, essas mensagens enfatizam a necessidade de serem repassadas rapidamente a um grande número de pessoas.

- Reenvios Anteriores: No corpo da mensagem, é possível notar cabeçalhos de e-mails que foram repassados por outras pessoas anteriormente.

Além disso, muitas vezes, uma pesquisa na Internet sobre o assunto da mensagem pode ajudar a localizar relatos e denúncias já feitas. É crucial não repassar boatos, pois ao fazê-lo, estará de alguma forma endossando ou concordando com o seu conteúdo.

Medidas Preventivas:

Aqui estão algumas dicas gerais para se proteger contra golpes online:

- Notificação: Se você identificar uma tentativa de golpe, é importante informar a instituição envolvida para que possam tomar as medidas adequadas.

- Mantenha-se Informado: Novos tipos de golpes podem surgir, portanto, manter-se informado é essencial. Algumas fontes de informação incluem:

- Seções de informática em jornais de grande circulação e sites de notícias, que frequentemente trazem matérias ou avisos sobre os golpes mais recentes.

- Sites de empresas mencionadas nas mensagens (algumas empresas colocam avisos em suas páginas quando percebem o uso indevido de seu nome).

- Sites especializados que divulgam listas de golpes em circulação e seus respectivos detalhes. Alguns desses sites incluem:

- Monitor das Fraudes (em português): http://www.fraudes.org/

- Quatro Cantos (em português): http://www.quatrocantos.com/LENDAS/

- TruthOrFiction.com (em inglês): http://www.truthorfiction.com/

- Urban Legends and Folklore (em inglês): http://urbanlegends.about.com/