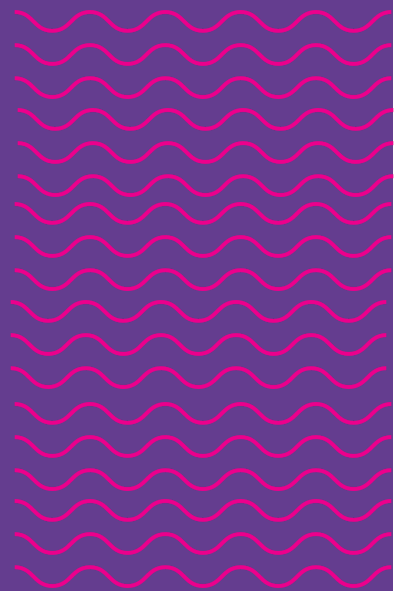
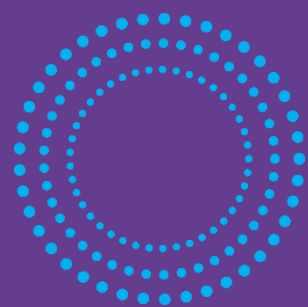
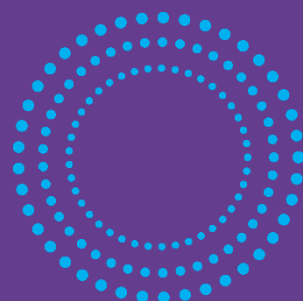
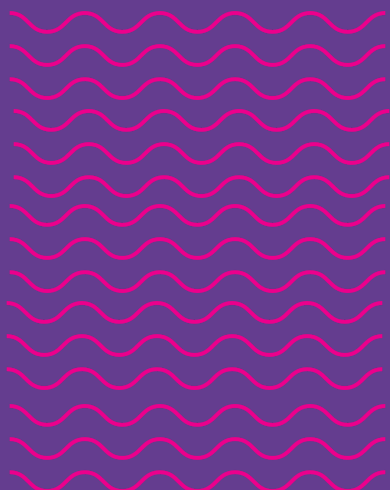




CARTILHA SEGURANÇA PARA INTERNET



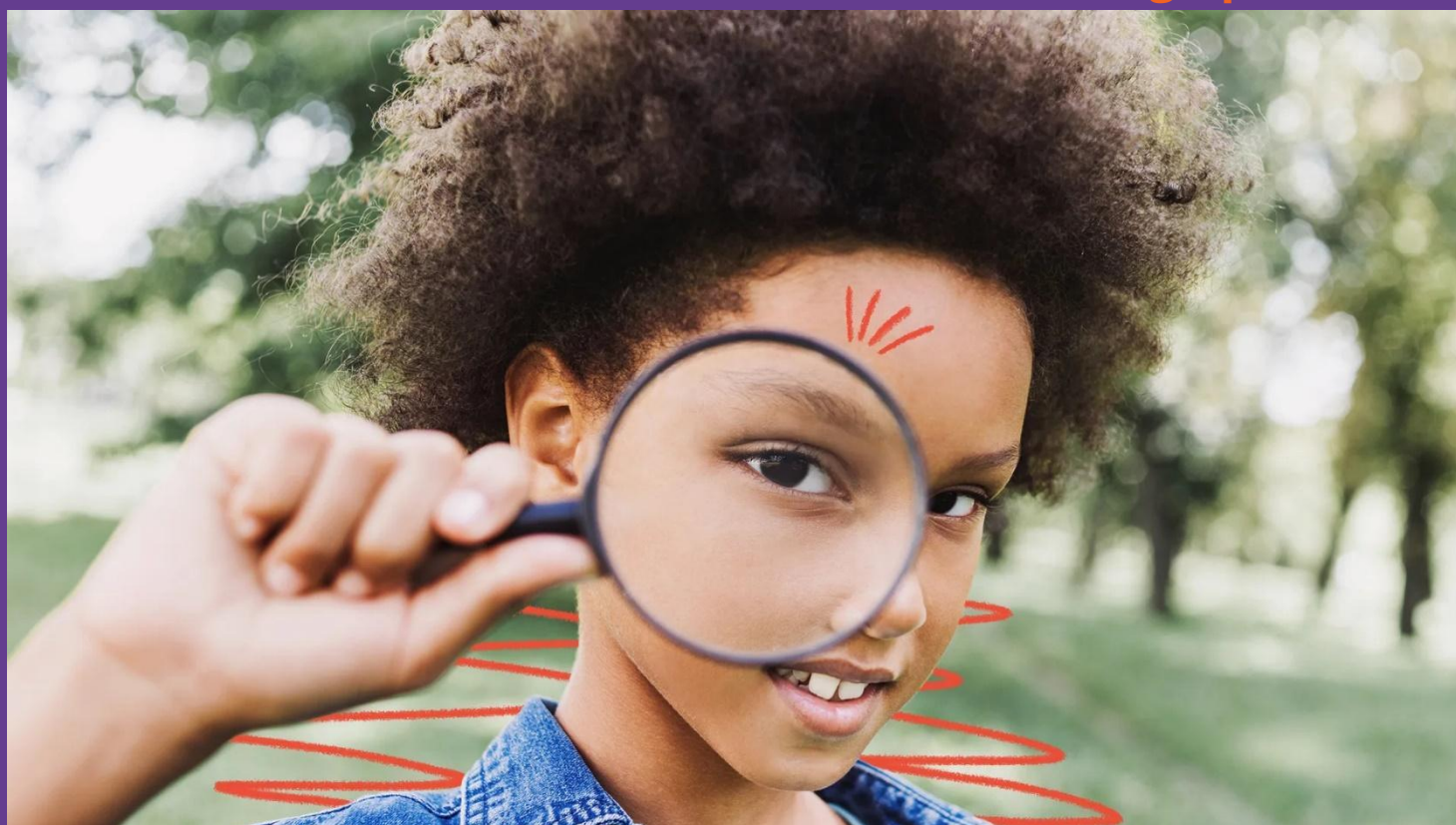
SUMÁRIO

Introdução.....	3
Furto de identidade.....	4
Fraude de Antecipação de recursos	5
Phising.....	6
Pharming.....	8
Golpes.....	9
Boatos.....	10
Falsificação de e-mail	10



1. INTRODUÇÃO

Olá querido(a) cliente, nós prezamos demais pela segurança dos seus dados e por isso criamos esse conteúdo, no intuito de te ajudar a ficar em alerta, diminuindo os riscos de cair em um golpe.



#OGolpeTaAi #FicaDeOlho

2. Furto de identidade (Identity Theft)

O furto de identidade, ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados

como crime contra a fé pública, tipificados como falsa identidade.

No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de e-mail e envie mensagens se passando por você ou falsifique os campos de e-mail, fazendo parecer que ele foi enviado por você.

Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser.

Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito.

Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

Como prevenir?

A melhor forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e as suas contas de usuário). Além disto, para evitar que suas senhas sejam obtidas e indevidamente usadas é muito importante que você seja cuidadoso, tanto ao usá-las quanto ao elaborá-las.

Fique atento à alguns indícios que podem demonstrar que a sua identidade está sendo indevidamente usada por golpistas, como:

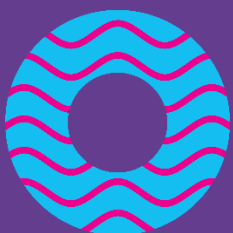
- Começar a ter problemas com órgãos de proteção de crédito;
- Receber retornos de e-mails que não foram enviados por você;
- Verificar nas notificações de acesso que a sua conta de e-mail ou seu perfil nas redes sociais foram acessados em horários/locais em que você próprio não estava acessando
- Ao analisar o extrato/fatura da sua conta bancária, você percebe transações que não foram realizadas por você
- Você recebe ligações, mensagens, e-mails referentes a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.

3. Fraude de antecipação de recursos (Advance fee fraud)



A fraude de antecipação de recursos, ou *advance fee fraud* é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Por meio de recebimento de mensagens



eletrônicas ou do acesso a sites fraudulentos, a pessoa é envolvida em alguma situação histórica ou mirabolante, que justifique a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado, para a obtenção de um benefício futuro. Após fornecer os recursos solicitados a pessoa percebe que o tal benefício prometido não existe, constata que foi vítima de um golpe e que seus dados e dinheiro estão em posse de golpistas.



O Golpe da Nigéria (Nigerian 4-1-9 Scam¹) é um dos tipos de fraude de antecipação de recursos mais conhecidos. Para ver mais sobre ele, você pode acessar [o site: https://noticias.r7.com/cidades/conheca-os-golpes-da-nigeria-e-saiba-se-proteger-24062015](https://noticias.r7.com/cidades/conheca-os-golpes-da-nigeria-e-saiba-se-proteger-24062015)

A fraude de antecipação de recursos possui diversas variações que, apesar de apresentarem diferentes discursos, assemelham-se pela forma como são aplicadas e pelos danos causados. Algumas exemplos são **oferta de emprego** (quando você recebe uma mensagem com uma proposta tentadora de trabalho mas para efetivar a contratação é necessário informar detalhes da sua conta bancária), **doação de animais** (você deseja adquirir um animal de uma raça bastante cara e, ao pesquisar por possíveis vendedores, descobre que há sites oferecendo estes animais para doação. Após entrar em contato, é solicitado que você envie dinheiro para despesas de transporte) e existem muitas outras variações desses golpes.

Como prevenir?

- Identificando mensagens contendo tentativas de golpes, com características como oferecimento de quantias de dinheiro, solicitação de sigilo, solicitação de resposta imediata, erros gramaticais e de ortografia;
- Adoção de uma postura preventiva questionando-se do “porque você entre milhares na internet foi escolhido pra receber um suposto benefício?”, desconfiar de situações que devem ser feitos pagamentos com promessas de futuramente receber o dobro do valor;
- Evitar de responder essas mensagens para não conter em históricos.

***Lembre-se: “Quando a esmola é demais o santo desconfia” ou “Tudo que vem fácil, vai fácil”.**

4. Phishing

É um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia. (A palavra phishing, do inglês *"fishing"*, vem de uma analogia criada pelos fraudadores, onde "iscas" (mensagens eletrônicas) são usadas para "pescar" senhas e dados financeiros de usuários da Internet).



O phishing ocorre por meio do envio de mensagens eletrônicas que tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, empresa ou site popular. Eles procuram atrair a atenção do usuário, seja por curiosidade, caridade ou possibilidade de obter alguma vantagem financeira.

Passam a informação de que a não execução dos procedimentos descritos podem acarretar em consequências como a inscrição em serviços de proteção de crédito, cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito. Eles tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição da instalação de códigos maliciosos, projetados para coletar informações sensíveis do preenchimento de formulários contidos na mensagem ou em páginas da Web.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento.

Veja alguns exemplos na tabela abaixo:

TO PICO	TEMA DA MENSAGEM
Comércio eletrônico	Cobrança de débitos, confirmação de compra, atualização de cadastro, devolução de produtos, oferta em site de compras coletivas
Companhias aéreas	Promoção, programa de milhagem
Eleições	Título eleitoral cancelado, convocação para o mesário
Empregos	Cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	Nova versão ou correção de programa Consulta de restituição, problema nos dados da declaração

Como prevenir?

1. Fique atento a mensagens recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;
2. Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco porque recadastrar dados ou atualizar módulos de segurança);
3. Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
4. Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
5. Seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador web;
6. Verifique o link apresentado na mensagem, golpistas costumam usar técnicas para ofuscar o link real para o phishing. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
7. Utilize mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antipshing;
8. Verifique se a página utiliza conexão segura. Sites de comércio eletrônico ou internet banking confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados;
9. Verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador web será diferente do endereço correspondente ao site verdadeiro;
10. Acesse a página da Instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

5. Pharming

Pharming é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de *DNS (Domain Name System)*. Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa. Esta redireção pode ocorrer:



- Por meio do comprometimento do servidor de DNS do provedor que você utiliza;
- Pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;
- Pela ação direta de um invasor, que venha a ter acesso as configurações do serviço de DNS do seu computador ou modem de banda larga.

Como prevenir?

- Desconfiar ao digitar uma URL e for redirecionado para outro site, o qual tenta realizar uma ação suspeita, como abrir um arquivo ou tentar instalar um programa;
- Desconfiar imediatamente caso o site de comércio eletrônico ou internet banking que você está utilizando não utilize conexão segura. Como já foi citado sites confiáveis de comércio eletrônico e internet banking sempre utilizam conexão segura quando dados sensíveis, pessoais e financeiros são solicitados;
- Observe se o certificado apresentado corresponde ao do site verdadeiro.

6. Golpes

Dentro do conteúdo, já foi possível verificar inúmeras formas de fraudes à segurança e além do que já vimos na internet também existem muitos tipos de golpes do comércio eletrônico (são aqueles nos quais golpistas com o objetivo de obter vantagens financeiras exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial), abaixo serão apresentados alguns desses.



#DICASDEPREVENÇÃO:

- Fazer uma pesquisa de mercado comparando os preços dos produtos expostos no site e caso os valores sejam muito abaixo dos encontrados na pesquisa, **desconfie!**
- Pesquisar na internet sobre o site antes de efetuar a compra, ver a opinião de outros clientes;
- Acessar sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a empresa (Exemplo: Reclame Aqui);
- Evite de informar dados de pagamento caso o site não ofereça conexão segura ou não apresente um certificado confiável.

#DICASDEPREVENÇÃO:

- Procure não fazer compras por impulso apenas para garantir o produto ofertado;
- Seja cauteloso e faça pesquisas prévias, pois há casos de produtos anunciados com desconto, mas que na verdade apresentam valores superiores aos de mercado;
- Pesquise sobre o site de compras coletivas antes de efetuar a compra para ver a opinião de outros clientes para observar se foi satisfatória a forma como os possíveis problemas foram resolvidos;
- Acessar sites especializados em tratar reclamações de consumidores insatisfeitos.
- Evite informar dados de pagamento caso o site não ofereça conexão segura ou não apresente um certificado confiável.

#DICASDEPREVENÇÃO:

- Marque encontros em locais públicos caso a entrega dos produtos seja feita pessoalmente sem transportadoras;
- Procure confirmar a realização de um pagamento diretamente em sua conta bancária ou pelo site do sistema de gerenciamento (não confie somente em e-mails, pois eles podem ser falsos);
- Acesse os sites diretamente pelo seu navegador.



7. Boato (Hoax)

Um boato, ou *hoax*, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Boatos podem trazer diversos problemas, tanto para aqueles que os recebem e os distribuem tanto para aqueles que são citados em seus conteúdos.

Entre os diversos problemas um boato pode: conter códigos maliciosos, espalhar desinformação pela internet, ocupar desnecessariamente espaço nas caixas de e-mails dos usuários, entre outras consequências.



Como prevenir?

- Conferindo a veracidade do conteúdo da mensagem, conferir a procedência, certifique-se de que não é um boato, uma fake news (notícia falsa).



8. Falsificação de e-mail (e-mail spoofing)

Falsificação de e-mail, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

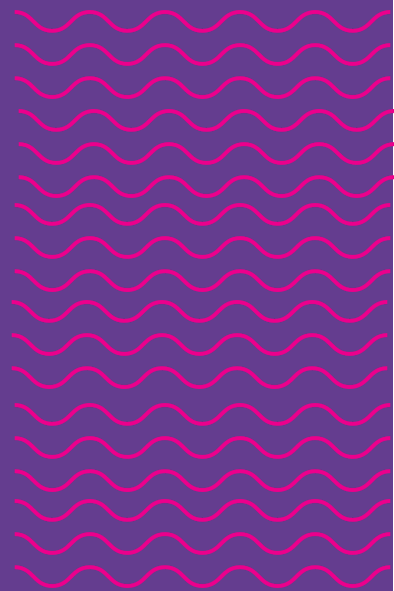
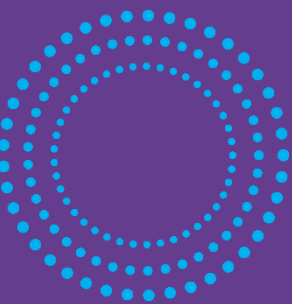
Essa técnica é possível devido a características do produto SMTP (Simple Mail Transfer Protocol) que permitem que campos de cabeçalho como "From" (endereço de quem enviou a mensagem) "Reply-To" (endereço de resposta da mensagem) e o "Return-Path" (endereço para onde possíveis erros no envio da mensagem são reportados) sejam falsificados.

Ataques desse tipo são bastante usados para propagação de códigos maliciosos, envio de spam e golpes de phishing. Atacantes utilizam-se de endereços de e-mail coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que eles partiram de pessoas conhecidas.

Exemplos de e-mails com campos falsificados são aqueles recebidos como sendo:

- De alguém conhecido, solicitando que você clique em um link ou execute um arquivo anexo;
- Do seu banco, solicitando que você altere dados da sua conta bancária.





#ProtejaSeusDados

