SEGURANÇA DIGITAL

Crimes cibernéticos
Recomendações

CIJUN
Companhia de Informática de Jundiaí

Introdução

Somos uma Companhia com quase 30 anos de atuação no mercado, especializada em tecnologias inovadoras para o desenvolvimento e integração de soluções de TIC (Tecnologia da Informação e Comunicação). Atendemos empresas dos setores público e privado e como resultado, temos conquistado o reconhecimento em prestigiadas premiações do setor. Contudo, nesse mundo moderno, nos preocupamos cada vez mais com a segurança digital do nosso cliente, do nosso parceiro, de seus funcionários e, principalmente, do cidadão comum.

Hoje em dia a Internet e os smartphones (com seus aplicativos móveis) se transformaram em um universo criativo, porém, perigoso e muito obscuro. Por conta disso, resolvemos elaborar uma Cartilha com alertas a alguns golpes que têm se tornado comuns. Mas não se engane: a cada dia surge um novo crime, por isso, essa Cartilha Digital será atualizada (de tempos em tempos) e estará disponibilizada em nosso site (www.cijun.sp.gov.br) para consulta. Nosso objetivo com essa iniciativa é orientá-lo pois temos como uma de nossas premissas, a responsabilidade social na inclusão digital do cidadão.

Companhia de Informática de Jundiaí

Veja exemplos de alguns golpes:

Clonagem de whatsapp

Mais de 5 milhões de pessoas caíram em algum tipo de golpe pelo WhatsApp no Brasil em 2020, revela um levantamento feito por um laboratório de segurança digital.

Os criminosos utilizam estratégias cada vez mais profissionais, usando o que os especialistas chamam de engenharia social. Eles iludem a vítima para conseguir o código de recuperação do WhatsApp e, assim, ter acesso aos dados pessoais das vítimas.

Esses golpes no WhatsApp são adaptados regularmente para fazer novas vítimas. Desde 2020, criminosos estão se aproveitando da pandemia provocada pelo coronavírus para aplicar golpes envolvendo o Auxílio Emergencial, por exemplo, benefício do Governo Federal criado com o intuito de diminuir os impactos provocados pela crise no País.

Além disso, o período também fez crescer o compartilhamento de golpes com phishing e fake news sobre a Covid-19, fraudes que podem continuar sendo exploradas neste ano de 2021.

Mas não se iluda: o criminoso é criativo e muda de tática todas as vezes que é descoberto.

Como se aplica a clonagem de whatsapp?

O criminoso liga ou envia uma mensagem se passando por um funcionário de site de compra ou de um banco e diz que estará encaminhando um código promocional ou código de confirmação. Ele pede para que a vítima informe esse código que, na verdade, é a verificação do WhatsApp e com ele o criminoso consegue clonar a conta do consumidor.

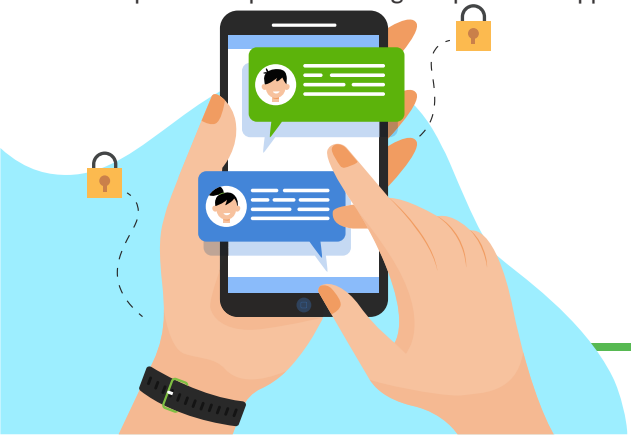
Após a clonagem, o criminoso passa a enviar mensagens para os contatos da vítima, se passando por ela, pedindo dinheiro. As desculpas para solicitar dinheiro emprestado são as mais diversas e, na maioria das vezes, os alvos principais da investida são os parentes mais próximos e amigos que, acreditando na mensagem, acabam depositando ou transferindo valores seguindo as coordenadas do criminoso.

Como evitar o golpe:

a) Ative a "Confirmação em duas etapas" no WhatsApp.
Acesse o link e veja como:
https://faq.whatsapp.com/general/verification/about-two-step-verification/?lang=pt_br

b) NUNCA forneça o código verificador que você recebe via SMS em seu celular.

c) Não instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém pelo whatsapp.



d) Desconfie de situações em que a pessoa solicita a realização de transferências e pagamentos em caráter de urgência.
e) Ligue para a pessoa que solicitou o dinheiro e verifique se realmente é ela quem está solicitando a transação.

Caso tenha sido vítima, o que fazer:

a) Envie um e-mail para support@whatsapp.com com o assunto "**CONTA HACKEADA – DESATIVAÇÃO DE CONTA**". Relate o ocorrido e siga as instruções do provedor.
b) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia na opção: OUTRAS OCORRÊNCIAS.
c) Peça para amigos e familiares excluírem o telefone clonado de grupos e alertarem o máximo de contatos em comum sobre o ocorrido.

Vítima foi quem fez o pagamento

a) Caso você tenha pago algo, entre em contato com o banco e tente bloquear o valor.
b) Providencie cópias ('prints') das conversas realizadas, bem como do comprovante de pagamento.
c) Em posse dessas informações, procure uma Delegacia de Polícia para o registro de Boletim de Ocorrência.

Aplicativo Espião

Outro golpe que tomou força no Whatsapp durante os últimos anos é a clonagem por meio de aplicativos espiões. Esses aplicativos parecem inofensivos, mas na realidade eles usam um sistema de spywares (ou stalkerwares) que basicamente abre a porta do seu telefone por alguma fresta, e o golpista pode ter acesso a uma série de informações pessoais, como conversas do WhatsApp, senhas de outras redes sociais, senhas de conta bancárias e até a localização do vítima em tempo real.

Esse tipo de coisa parece assustador, mas a cada dia que passa, isso tem se tornado cada vez mais comum. Com a intenção de monitorar as atividades de seu cônjuge, aqueles parceiros ciumentos instalam esse malware no celular da vítima e, a partir disso, consegue monitorar cada atividade da pessoa. Nesse caso, a pessoa só consegue realizar a instalação desse invasor de forma física, ou seja, o golpista tem que estar com o celular da vítima em suas mãos.

Mas além dos parceiros ciumentos, existem também os ataques hackers que geralmente enviam o malware através de phishing e, sem saber do que se trata, a própria vítima instala o aplicativo espião no celular. Independente de como seja instalado, com o objetivo de monitorar o parceiro ou roubar os dados pessoais, usar aplicativo espião está previsto em lei e é crime.

Solução: Novamente, para evitar o acesso ao seu smartphone por meio de um malware, nada mais útil que um antivírus capaz de identificar ameaças instaladas no seu celular. Esses aplicativos agem em tempo real e costumam te notificar sobre o risco que você pode estar correndo.

Dicas importantes:

Links maliciosos: 'Saque do FGTS', entrega grátis de um 'super almanaque da Turma da Mônica', acesso vitalício à 'Netflix' ou 'Spotify' de graça, e até 'vagas de emprego' foram tipos de links utilizados para afetar as vítimas.

NUNCA ACREDITE EM VANTAGENS ASSIM!

Esse tipo de golpe pode ser evitado se você tiver um antivírus instalado em seu smartphone, até porque esse programa tem monitoramento em tempo real que consegue identificar o que é uma ameaça phishing. Além do antivírus é necessário atenção, até porque o melhor antivírus é você!

Então, suspeite de promoções que são boas demais e jamais clique nesses links suspeitos, por mais que tenham sido encaminhados por pessoas de confiança, ou até em grupos de amigos ou família. Se você criar essa prática, em determinado momento, só de olhar, você vai conseguir identificar se é um link suspeito ou não.

Boleto falso

O boleto de cobrança é um instrumento de pagamento pelo qual o emissor, denominado "Beneficiário", receberá em sua conta o valor referente a um produto ou serviço. O criminoso, valendo-se de engenharia social ou de um link fraudulento, altera o código de barras de modo que o valor caia na conta do integrante da quadrilha.

Segundo a Federação Brasileira de Bancos (Febraban), aumentou em 45% o número de golpes durante a pandemia do novo coronavírus. Fraudes relacionadas a boletos bancários são uma preocupação antiga do setor. A prática envolve a falsificação de cobranças para fazer com que o pagamento vá para a conta bancária do golpista. São vários truques para

atrair a vítima, que vão desde a manipulação do código de barras do documento até a criação de páginas falsas que oferecem o download da fatura forjada.

Como evitar o golpe:

a) Verifique se os dados do "Beneficiário" correspondem aos de quem lhe vendeu o produto ou serviço.

b) Confira se os três primeiros números do código de barras correspondem ao banco cuja logomarca aparece no boleto.

c) Desconfie se o código de barras estiver com falhas que apresentem espaços excessivos entre as barras ou qualquer outra alteração que impossibilite o reconhecimento pela leitora.

d) Sempre que tiver dúvidas sobre a veracidade de um boleto de cobrança, consulte diretamente o fornecedor que o emitiu.

e) Evite reimprimir boletos de cobrança em sites que não sejam do banco emissor do boleto. Evite negociar valores de descontos de boletos com pessoas estranhas, ou que se identificam como funcionários dos bancos ou de empresas de cobrança.

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.

b) Tire cópia do comprovante de pagamento e demais documentos correlatos.

c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia na opção: OUTRAS OCORRÊNCIAS.

Fraudes bancárias

Os golpes de phishing bancário estão crescendo no Brasil e já atingiram mais de dez milhões de pessoas em 2020. Em relação ao mesmo período em 2019, é possível perceber um aumento de 43% no número total de ataques.
Então, atente-se:

Alguns meios:

Phishing:

O criminoso envia links, e-mails e SMS para a vítima com mensagens que, na maioria das vezes, exploram as emoções (curiosidade, oportunidade única, medo, etc), fazendo com que ela clique nos links e anexos que subtraem dados pessoais ou induzem a realizar cadastros ou fornecer informações.

Falso funcionário ou falsa central de atendimento:

O estelionatário finge ser funcionário da instituição financeira e diz estar com problemas no cadastro ou irregularidades na conta. A vítima fornece informações sobre sua conta, e com isso o bandido realiza transações fraudulentas.

Falso motoboy:

Integrantes da quadrilha ligam para a vítima e dizem pertencerem à central de relacionamento do banco. Afirmam que houve problemas com o cartão da vítima e pedem que ela digite sua senha numérica no teclado do telefone. Na sequência, dizem que enviaram um motoboy na casa da vítima para pegar o cartão. Em posse do cartão e a senha, operações espúrias.

Falso leilão

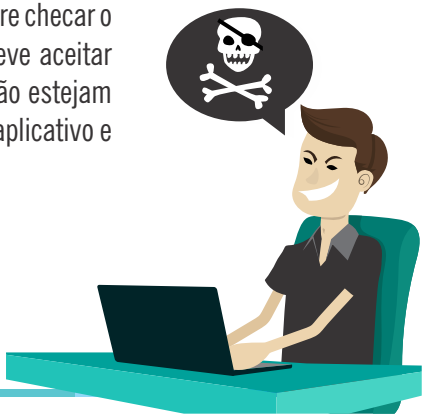
Neste caso, o fraudador envia um link que simula um leilão falso, no qual a vítima precisa fornecer dados pessoais e financeiros, além de depositar um valor na conta do criminoso. Com o CPF, a senha e o número do cartão da pessoa, é possível fazer qualquer tipo de transação em nome do cliente.

Extravio do cartão:

Durante o processo de entrega do cartão, a correspondência é furtada e, então, o criminoso liga para a vítima fingindo ser um funcionário do banco informando que aconteceram problemas na entrega. Eles solicitam a senha do cartão para resolver o suposto problema e realizam transações em nome da pessoa. A Febraban, no entanto, ressalta que o cliente nunca deve enviar dados, senhas e acessos a ninguém. Também nunca deve preencher formulários na internet com dados pessoais e financeiros sem verificar a origem. "Caso o prazo de entrega do cartão se esgote, é preciso informar o gerente sobre o atraso", diz.

Golpe do delivery:

Esse é outro golpe famoso que vem sendo aplicado durante a pandemia. Nele, o entregador apresenta uma maquininha com o visor danificado e cobra um valor acima do que foi cobrado pelo restaurante. Como evitar: "O cliente deve sempre checar o preço cobrado no visor da maquininha e nunca deve aceitar maquininhas onde os valores que são cobrados não estejam visíveis. De preferência em fazer o pagamento via aplicativo e não no momento da entrega", diz a Febraban.



Como evitar o golpe:

a) Evite usar computadores públicos e redes abertas de wi-fi para acessar conta bancária ou fazer compras online.
b) NUNCA abra e-mails de origem ou de procedência duvidosa.
c) Não execute programas, abra arquivos ou clique em links que estejam anexados ou no corpo desses e-mails.
d) Delete esses e-mails e, caso tenha clicado em alguma parte deste e-mail e executado um programa, comunique imediatamente ao seu banco o ocorrido e altere todas as suas senhas de acesso à sua conta bancária em outro computador confiável, ou no mesmo, após uma verificação completa de infecção de vírus por um técnico confiável;
e) NUNCA utilize seu cartão para fazer compras em sites desconhecidos.

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica: https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia na opção: OUTRAS OCORRÊNCIAS.

Sites de comércio eletrônico fraudulentos

Dados da ferramenta "Transparency Report", do Google, mostram que em temporadas normais, o número de sites que parece legítimo para fazer os usuários digitarem informações pessoais não passa da casa dos 40 mil ao redor do mundo.
No entanto, desde que a pandemia de coronavírus ganhou força, esse cenário mudou de cara: a ferramenta apontou em

2020, 159.3 mil sites inseguros. Nessa modalidade, o golpista cria uma página na internet muito semelhante à verdadeira, e levando a vítima a acreditar que está efetuando uma compra legítima. Após selecionar os produtos e efetuar o pagamento, a vítima não recebe a mercadoria, quando então percebe que caiu em um golpe.

Para aumentar as chances de sucesso, o estelionatário utiliza artifícios, tais como: envio de spams, oferta de produtos com valor abaixo do valor de mercado, propagandas através de links patrocinados, dentre outros. Além do comprador, as empresas que tiveram seus nomes utilizados indevidamente, ou ainda, as pessoas que tiveram seus dados utilizados para criação do site ou para a abertura de "empresas fantasmas", também são vítimas.

Como evitar o golpe:

Algumas dicas são indispensáveis, para que possamos ter a certeza que estamos fazendo uma compra legítima, com segurança:

a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;

b) Leia atentamente as informações dos sites e do produto que deseja comprar. Normalmente, sites fraudulentos podem conter erros de português ou ainda sobre as informações técnicas do produto. Verifique também se há CNPJ cadastrado na página ou canais de comunicação;

c) Faça uma pesquisa de mercado do valor do produto que deseja adquirir. Desconfie de preços muito baixos;

d) Realize pesquisas na internet para obter informações a respeito da reputação do site em que deseja efetuar compras. Essas informações podem ser obtidas através do https://www.reclameaqui.com.br/ ou de redes sociais.

É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon:
(https://www.procon.sp.gov.br/)

e) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;

f) Evite clicar em links que direcionam a navegação diretamente ao site de compras. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador.

Atenção: os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro.

Exemplo fictício:

https://www.americanas.com.br/ (site verdadeiro)
https://www.lojasamercanas.com.br/ (site falso).

Note que no exemplo do site falso foi incluído o nome "lojas" e a letra "i" do nome "americanas" foi suprimida.

Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);

b) Faça um print da página e do produto anunciado;

c) Providencie uma cópia do boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;

d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica: https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia na opção: OUTRAS OCORRÊNCIAS.

"RANSONWARE" (sequestro de dados)

Segundo o The State of Ransomware 2020, feito pela Sophos (uma desenvolvedora e fornecedora de software e de hardware de segurança), em 2019, 65% das organizações brasileiras pesquisadas sofreram um ataque ransomware. Apenas 36% delas conseguiram bloqueá-los antes de os dados serem criptografados. Em 2020, só no primeiro semestre, o aumento nos ataques no mundo foi de 72%, segundo levantamento da Skybox Security, empresa também especializada em segurança.

Já segundo dados da Kasperski (empresa tecnológica russa especializada na produção de softwares de segurança para a Internet), o ano de 2020 teve um aumento de 350% nos ataques ransomware no primeiro trimestre. Ainda de acordo com a organização, o Brasil figura no topo dos países mais afetados no mundo por ataques desse tipo. De acordo com as análises citadas, esse aumento nos ataques se deve sobretudo à ida tão repentina quanto maciça para o home office e pela própria pandemia, grande motivo de e-mails e mensagens phishing.

O golpe ocorre da seguinte forma:

O ransomware é um vírus que "tranca" os seus dados até o pagamento de um resgate.

Na maioria das vezes a invasão ocorre no período da noite ou madrugada, momento em que um criminoso virtual invade o dispositivo da vítima e instala um software capaz de criptografar (codificar) as informações de seu computador. Ao acessar o computador após tal procedimento, a vítima receberá uma mensagem de que seus dados foram criptografados e se ela não realizar um pagamento exigido pelo criminoso, normalmente em bitcoins, a vítima perderá todos os dados do computador invadido.

Como evitar o golpe:

a) Mantenha backup atualizado do computador, de preferência em HD externo ou pen drive e nunca os deixe espetados no computador, pois também poderão ser invadidos ou infectados;
b) Mantenha antivírus e firewalls sempre ativados e atualizados;
c) Evite acesso a sites suspeitos;
d) Não clique em links duvidosos de e-mails suspeitos.

Caso tenha sido vítima, o que fazer:

a) Não apague os e-mails e/ou mensagens recebidas do criminoso;
b) Se houver conversa com o criminoso via rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias, inclusive carteiras eletrônicas de bitcoins informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia na opção:
OUTRAS OCORRÊNCIAS.

Golpes envolvendo PIX

As recomendações com relação às transações PIX são, em geral, as mesmas para o acesso a serviços financeiros já utilizados, como TED e DOC.

Não entre em sites ou instale no celular aplicativos desconhecidos; Não há sites ou aplicativos do Banco Central ou do Pix criados exclusivamente para cadastramento das chaves, nem para a realização das transações Pix;

O cadastramento das chaves é realizado em ambiente logado no aplicativo ou site da sua instituição de relacionamento, o mesmo que já é utilizado para as demais transações financeiras, como consultar saldo, fazer transferências ou tomar dinheiro emprestado;

O cadastramento das chaves requer o consentimento do cliente e para cadastrar a chave Pix é feita uma validação em duas etapas. O cadastro do número de celular ou do e-mail como chave Pix depende da confirmação por meio de um código que será enviado, por exemplo, por SMS ou para o e-mail informado.

Já o CPF/CNPJ só pode ser usado como chave se estiver vinculado à conta, informação necessária no momento de sua abertura, comprovada por meio de documento.

Se o usuário tem dúvidas, procure se informar através do site da sua instituição de relacionamento.

Não há prazo para o cadastramento das chaves que começou em 05 de outubro de 2020 e estará sempre disponível.

Caso tenha sido vítima, o que fazer:

a) Reunir toda documentação da transação (extratos, comprovantes, etc)
b) Registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica:
https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia na opção:
OUTRAS OCORRÊNCIAS ou registre os fatos presencialmente no Distrito Policial mais próximo da residência.
c) Cientificar o prestador de serviço de pagamento para eventual ressarcimento, após análise dos documentos.

FONTES

Polícia Civil de SP - https://www.policiacivil.sp.gov.br/
Oficina de Net - https://www.oficinadanet.com.br/
Olhar Digital - https://olhardigital.com.br/
Jornal "O Estado de SP" - https://www.estadao.com.br/
Isto É Dinheiro - https://www.istoedinheiro.com.br/
RTM Telecom - https://www.rtm.net.br/
CNN Brasil - https://www.cnnbrasil.com.br/

CIJUN
Companhia de Informática
de Jundiaí

www.cijun.sp.gov.br
30 ANOS | 2021

03/21
V 01

comunicação
cijun