

Como agir em casos de

CRIMES VIRTUAIS

Editoração: Lucca Melo
Agência LUM

Crimes Virtuais

Hoje são cada vez mais comuns ocorrências como o hackeamento de contas, a divulgação de sites e boletos falsos. Nessa cartilha você vai conhecer medidas para fazer cessar ou minimizar danos causados por condutas criminosas, como a interrupção de comportamento viral de fake news, conteúdo impróprio ou criminoso nos meios digitais. E também receberá orientações práticas de prevenção.

Muitas relações e vínculos são criados e desenvolvidos nos ambientes virtuais, principalmente nas redes sociais.
No entanto, os avanços tecnológicos que permitem essa interação são os mesmos utilizados por cibercriminosos para fazer ataques virtuais com o objetivo de dar golpes e realizar fraudes eletrônicas. Por isso, é essencial tomar medidas para proteger os dados expostos na internet.

Fontes:
Cartilha Prevenção contra invasões e crimes informáticos (Tribunal de Justiça do Estado de Minas Gerais)
Guia de orientações e prevenção a golpes (Ministério da Defesa)

Clonagem de contas no WhatsApp

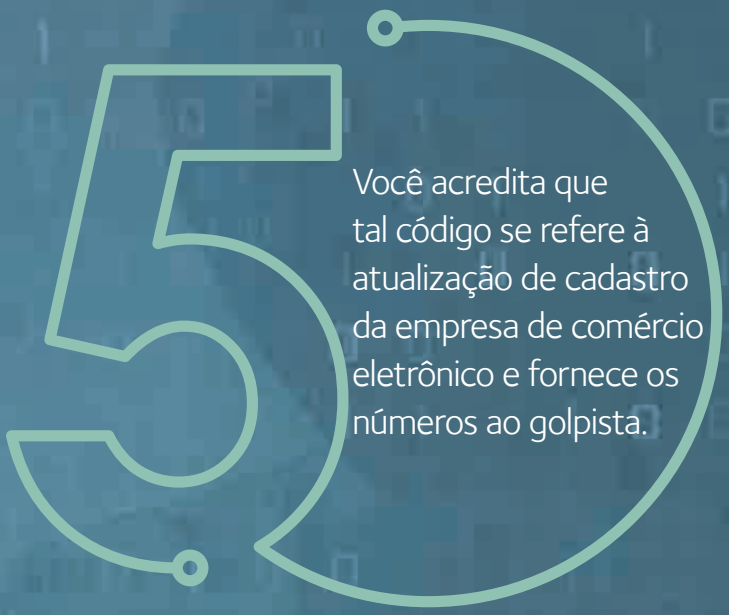
1. Você anuncia um produto em sites de comércio eletrônico e divulga o número de telefone para contato.

2. O golpista envia uma mensagem para o seu WhatsApp, comunicando ser da empresa de comércio eletrônico e solicita a atualização de dados cadastrais.

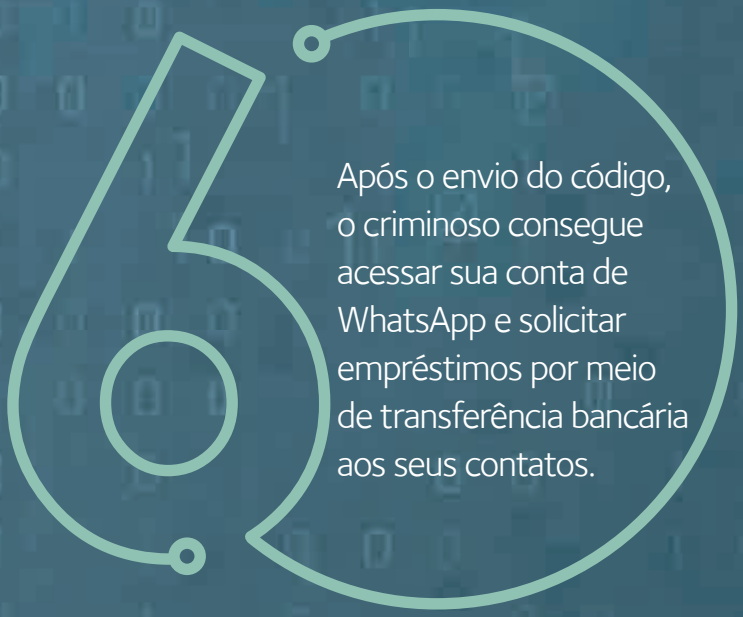
3. Requer, na ocasião, que seja fornecido o código de 06 dígitos enviado por SMS.

4. Na verdade, o golpista está tentando acessar seu WhatsApp por meio do número vinculado à sua conta, sendo necessário, para tanto, utilizar o código de **06 dígitos** enviado por SMS.

Clonagem de contas no WhatsApp

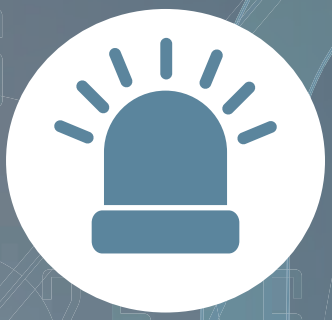


Você acredita que tal código se refere à atualização de cadastro da empresa de comércio eletrônico e fornece os números ao golpista.



Após o envio do código, o criminoso consegue acessar sua conta de WhatsApp e solicitar empréstimos por meio de transferência bancária aos seus contatos.

Orientação para recuperação de contas



Registrar Boletim de Ocorrência



Enviar e-mail para support@whatsapp.com.
No assunto, escrever: "Perdido/Roubados: Por favor, desative minha conta". No corpo da mensagem, colocar o número do telefone com o código do país.
Ex: +55 99999-9999.

A empresa WhatsApp irá desativar a conta, que só poderá ser utilizada após **07 dias**.

Caso o golpista tenha habilitado verificação em duas etapas, você deverá reinstalar o número no aplicativo e digitar aleatoriamente códigos sucessivos, a fim de acarretar a suspensão da conta por um prazo de 07 dias. Após o período, você receberá um novo SMS com o novo código de ativação.



QRL Jacking
Espelhamento indevido do WhatsApp
Como funciona?

Phishing é uma maneira desonesta que cibercriminosos usam para enganar a vítima para que ela revele informações pessoais, como senhas de cartão de crédito/débito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando o usuário a websites falsos.



No caso de espelhamento do WhatsApp, os criminosos criam páginas bem elaboradas de phishing, com QR Coding do WhatsApp, permitindo que capturem a sessão do aplicativo quando você faz o login por meio do WhatsApp Web ou Desktop.

Você utilizará normalmente o WhatsApp pelo smartphone, enquanto o criminoso terá acesso ao aplicativo pelo WhatsApp Web, conseguindo acessar suas conversas com seus contatos.

Dicas de prevenção

- Não escanear o QR Code do celular em sites desconhecidos.
- Acessar o aplicativo apenas pelo WhatsApp Web ou na versão Desktop.
- Evitar utilizar o WhatsApp Web em conexões públicas ou pouco confiáveis.
- Verificar, com frequência, as sessões ativas do smartphone. Para tanto, em telefone IOS, siga o seguinte passo: abra o aplicativo: *Ajustes>WhatsApp Web/Desktop>Dispositivos com sessões ativas. Já nos aparelhos com sistema Android, faça o seguinte: abra o aplicativo>clique em "..." no canto superior da tela>WhatsApp Web>Sessões Ativas.*
- Por fim, lembrar sempre de manter a versão do WhatsApp atualizada.

Hackeamento de conta do Instagram
Perda de acesso

Como proceder em caso de perda de acesso?

1. Acesse a conta de e-mail vinculada ao Instagram e localize a mensagem, informando a modificação.
2. Desfaça, caso possível, a modificação de senha.

Dicas de prevenção

- Usar senha distinta para acessar o Instagram e o e-mail vinculado.
- Habilitar verificação em duas etapas.

Outros procedimentos para recuperação de acesso da conta do Instagram

Invasão criminosa – Após o registro da ocorrência, a autoridade policial poderá requisitar a recuperação da conta.

Evento não criminoso – Denunciar a conta.
Android: na tela de login, clicar em "Obter ajuda para entrar.
IOS: na tela login, clicar em "Esqueceu a Senha?"

Bolware
Fraudes por alteração de boleto bancário



Bolware é o malware instalado no seu computador para a modificação dos dados de criação e pagamento do boleto bancário. Quando você gera o documento para pagamento por meio de um computador infectado, o malware altera a linha digitável, fazendo com que os valores sejam repassados para conta de terceiros e não do verdadeiro cedente/beneficiário.

Como se proteger?

- Mantenha antivírus e sistema operacional atualizados.
- Evite abrir links de terceiros e anexos de e-mails de fontes desconhecidas.
- Observe todas as informações do boleto.
- Dados sobre as instituições financeiras podem ser consultados por meio do site Busca da FEBRABAN (http://www.buscabanco.org.br/).
- O boleto deve ter nome e logomarca do banco emissor coincidentes.
- O número do banco e os 03 (três) primeiros caracteres da linha digitável devem ser iguais, pois esses números são destinados à identificação do banco.
- Independentemente do banco emissor do boleto, a linha digitável deve conter a agência, o código cedente e, ao final, o valor do documento.



Fraude eletrônica por RAT bancário (Remote Acess Trojan)

O RAT bancário, “Trojan de Acesso Remoto” ou Remote Acess Trojan, é o malware utilizado pelos criminosos para assumir o controle do seu computador, subtrair credenciais de acesso de Internet Banking e desviar valores de contas sem seu conhecimento.



Na prática, executa ações de programas legítimos e age como se estivesse utilizando fisicamente o seu computador.

Dicas de prevenção

- Manter o antivírus e sistema operacional atualizados.
- Evite abrir anexos de e-mails de fontes não confiáveis.
- Desative portas não utilizadas.
- O firewall deve estar ativado e configurado adequadamente.

Como funciona a fraude

1 Envio do RAT

O criminoso envia o RAT por meio de anexos de e-mail, links maliosos, programas ou aplicativos com malwares ocultos baixados por você.

2 Abertura

Acreditando se tratar de algo de seu interesse, você abre e executa o RAT, dando aos criminosos acesso e controle ao seu dispositivo.

3 Desvio de dinheiro da conta

Já com acesso ao seu dispositivo, os criminosos acessam suas credenciais e senhas do Internet Banking ou do aplicativo do banco, desviando valores de suas contas.



Se receber um e-mail, SMS ou mensagens em seu celular com link, fique atento!

Veja como verificar se a comunicação é de fonte legítima e se o link é seguro para clicar:

- Confira se o remetente do e-mail é o oficial.
- Antes de clicar em um link, passe o mouse sobre ele e veja se você será direcionado para a página oficial do remetente.
- Desconfie de comunicações que solicitem seus dados pessoais e nunca informe senhas.
- Entre em contato com seu banco para relatar qualquer problema ou suspeita de fraude. No caso do Santander, se receber uma comunicação suspeita, envie a evidência para suspeita@santander.com.br.

Typosquatting - "sequestro" de URL



É normal abrir o navegador e, por algum equívoco, digitar erradamente o nome do domínio que se pretende acessar. Aproveitando-se dessa situação corriqueira, os criminosos criam sites fraudulentos, praticamente idênticos ao site verdadeiro, para enganar os usuários.

Em suma, os criminosos normalmente pretendem o seguinte:
a) praticar fraudes eletrônicas (ex.: vender produtos e não realizar a entrega);
b) vender domínio ou redirecionar tráfego para concorrente;
c) compartilhar fake news;
d) monetizar páginas com publicidade.

Golpes comuns

Passagem aérea - O estelionatário vende uma passagem aérea com preço muito abaixo do de mercado, alegando ser fruto de bônus de cartão de milhagem. A vítima compra-a e, no momento do embarque, ocasião em que é solicitada a identidade, é notificada que a passagem foi adquirida com cartão roubado, sendo impedida de realizar a viagem e acusada de conluio no golpe.





Mensagem premiada via celular
Estelionatário envia mensagem para o celular da vítima, informando que ela ganhou um prêmio e que para recebê-lo deverá depositar uma quantia em dinheiro na conta corrente do golpista.

Ingressos falsos - O golpe é aplicado através de promoções de ingressos ofertados nos sites para diversos shows e/ou eventos, tais como: UFC; shows de artistas; viagens em cruzeiros; copa das confederações; copa do mundo; etc...



ArcelorMittal

Regras básicas de proteção contra golpes

- Nunca aceite ajuda de estranhos, especialmente em bancos.
- Não forneça ou confirme dados particulares por telefone, pois você não sabe quem está do outro lado da linha.
- Jamais reaja a assaltos ou sequestros.
- Cuidado com sua documentação pessoal.
- Desconfie de ofertas generosas.
- Procure tratar pessoalmente assuntos com as instituições financeiras credenciadas.
- Nunca deposite dinheiro na conta de desconhecidos.
- Nunca guarde o cartão e a senha no mesmo lugar.
- Nunca compartilhe suas senhas com outras pessoas.
- Não compartilhe dados pessoais (sobretudo bancários) com terceiros.
- Não repasse códigos que receber por SMS.
- Sempre que receber alguma ligação, e-mail ou mensagem de algum serviço que você possui (como banco ou operadora de telefonia), desligue e entre em contato com um canal oficial da empresa.
- Nunca abra links de remetentes que geralmente não enviam e-mails e/ou links e/ou arquivos para você. Se tiver alguma dúvida, contate o remetente para verificar se foi realmente ele que compartilhou tais links ou arquivos.
- Nunca forneça suas credenciais para acessar conteúdos através de um link.

- Não conceda seus dados para descobrir se seus dados foram vazados.
- Fique atento a mensagens, e-mails e SMS que informem códigos para verificação de conta sem que você tenha solicitado e nunca os informe para ninguém, pois, através deles, muitos criminosos tentam fazer a clonagem dos sites e mídias sociais.
- Acompanhe diariamente os extratos de sua conta bancária e do cartão de crédito.
- Monitore a movimentação do seu cadastro no SPC/Serasa.
- Consulte se há linhas telefônicas pré-pagas ativas em seu CPF no sistema da ANATEL: https://cadastropre.com.br/#/consulta
- Consulte no site do Banco Central se há vínculo com instituições financeiras que você desconheça: https://www.bcb.gov.br/cidadaniafinanceira/registrato
- Se tiver sido vítima de alguma fraude, notifique a Autoridade Nacional de Proteção de Dados Pessoais no link: https://www.gov.br/anpd/pt-br

Remoção de conteúdo

Caso algum conteúdo de cunho íntimo, infamante ou violador de direitos seja exposto na internet sem a sua autorização, poderão ser adotadas as seguintes medidas:

Exclusão de conteúdo sem ordem judicial

Em redes sociais e plataformas de conteúdo digital, como Facebook, Twitter e Youtube, é possível denunciar diretamente o conteúdo postado. Você poderá optar por uma notificação extrajudicial ou ofício de autoridade policial.

A remoção é obrigatória e independe de ordem judicial se envolver compartilhamento de conteúdo íntimo, cenas de nudez ou de atos sexuais de caráter privado, sem autorização.

O art. 19 do Marco Civil da Internet dispõe que a exclusão de conteúdo postado na internet, em regra, necessita de ordem judicial.

A ordem judicial deverá conter identificação clara e específica do conteúdo apontado como infringente que permita a localização inequívoca do material.

Outra opção que pode ser utilizada é a desindexação de conteúdo, isto é, a remoção do conteúdo dos resultados de mecanismos de busca (Google e Bing), que pode ser determinada judicialmente para remover informações pessoais dos resultados de pesquisas, tais como: RG, conta bancária, cartão de crédito, imagem de assinatura manuscrita, imagem ou vídeo sexualmente explícito que tenha sido distribuído sem consentimento.

Interrupção de conteúdo viral no WhatsApp

É cada vez mais comum o compartilhamento de fake news, conteúdo impróprio ou criminoso nos meios digitais, sobretudo envolvendo autoridades ou pessoas públicas.



É possível, porém, a suspensão de vídeos, áudios e imagens encaminhadas por usuários ou grupos na plataforma. Com a identificação da URL de encaminhamento, ordem judicial poderá determinar a interrupção do comportamento viral.

Como identificar a URL de encaminhamento

1 Utilizar o Mozilla Firefox.
2 Abra o Whatsapp Web.
3 Crie um grupo para encaminhamento do conteúdo.
4 Abrir o menu na parte superior do navegador.
5 Disable cache – Marcar All e clicar na lixeira.
6 Carregue o conteúdo no grupo para encontrar a URL.
7 Identifique a URL com o final .enc.
8 Instruir pedido na Justiça, constando a URL do conteúdo a ser suspenso.

Informações relevantes para o registro de ocorrência policial



Informação obrigatória

Informar data, hora e local do último acesso, com redes wifi ou conexões de internet utilizadas, conta de e-mail vinculada e, ainda, relatos da conta utilizada pra postagens ou envio de e-mail.

Dispositivos informáticos

Indicar os dispositivos informáticos utilizados para acessar a conta (ex: celular, notebook, computadores, etc) e se existia acesso em computadores de terceiros. Em perda de acesso em ocasiões anteriores, relatar o fato e as circunstâncias.

Senhas

Indicar os dispositivos informáticos utilizados para acessar a conta (ex: celular, notebook, computadores, etc) e se existia acesso em computadores de terceiros. Em perda de acesso em ocasiões anteriores, relatar o fato e as circunstâncias.

Arquivos suspeitos

Informar se houve acesso a sites suspeitos, instalação de softwares distintos ou cliques em links duvidosos.

Denúncia

Informar se houve denúncia diretamente no provedor de e-mail ou na rede social sobre a perda de acesso ou hackeamento.