PREVENÇÃO CONTRA INVASÕES E CRIMES INFORMÁTICOS

CARTILHA PARA MAGISTRADOS E SERVIDORES DO TRIBUNAL DE JUSTIÇA DO ESTADO DE MINAS GERAIS

TJMG


APRESENTAÇÃO

O mundo virtual, a vida virtual e a necessidade de estar conectado em tempo real em todos os momentos são uma constante na sociedade atual. Os momentos privados cotidianos são retratados nas redes sociais como se fizessem parte de uma vida social virtual. Muitas relações e vínculos sociais são criados e desenvolvidos nesse meio.

Os avanços tecnológicos que permitem essa interação, no entanto, trazem consigo novos desafios, notadamente, as providências e precauções a serem tomadas para proteção de dados expostos na internet.

Desde julho de 2018, a Assessoria da Polícia Civil do TJMG (ASPC 2ª Instância) vem registrando ocorrências policiais, colhendo relatos e acompanhando inúmeras fraudes eletrônicas cometidas contra magistrados e servidores deste Tribunal.

No cenário nacional, matérias jornalísticas noticiaram recentemente que aparelhos telefônicos de diversas autoridades dos Poderes da República haviam sido clonados e suas conversas íntimas interceptadas e expostas ao público em um site. As invasões aos aparelhos telefônicos objetivaram capturar diálogos entre membros do Ministério Público, juízes, desembargadores e ministros, entre outros, a respeito dos processos judiciais da denominada “Operação Lava-Jato”.

Essa ação criminosa revelou a fragilidade da segurança das conversas privadas travadas em aplicativos de mensagens e demonstrou também que autoridades do Poder Judiciário estão, cada vez mais, no “radar” de criminosos virtuais.

Diante desse preocupante cenário é que decidimos elaborar a presente cartilha, que, com linguagem simplificada, objetiva apresentar aos magistrados e servidores do Tribunal de Justiça algumas das recentes fraudes eletrônicas realizadas por cibercriminosos, a fim de que se previnam contra possíveis ataques virtuais. Além disso, procuramos apontar medidas que podem ser adotadas para fazer cessar ou minimizar os danos causados por determinadas condutas criminosas, como a interrupção de comportamento viral de *fake news*, conteúdo impróprio ou criminoso nos meios digitais.

Portanto, sem qualquer pretensão de esgotar a temática, esperamos que a presente cartilha possa disseminar, no âmbito do Poder Judiciário mineiro, algumas orientações práticas de prevenção contra invasões e crimes informáticos.

Guilherme Siqueira Batista
Delegado de Polícia, Chefe da Assessoria da Polícia Civil do TJMG

CLONAGEM DE CONTAS NO WHATSAPP

1. A vítima anuncia um produto em sites de comércio eletrônico e divulga o número de telefone para contato.
2. O golpista envia uma mensagem para o Whatsapp do anunciante, 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 o Whatsapp da vítima por meio do número vinculado à conta, sendo necessário, para tanto, utilizar o código de 06 dígitos enviado por SMS.
5. A vítima acredita que tal código se refere à atualização de cadastro da empresa de comércio eletrônico e fornece os números ao golpista.
6. Após o envio do código, o criminoso consegue acessar a conta de Whatsapp da vítima e solicitar empréstimos por meio de transferência bancária aos seus contatos.

ORIENTAÇÕES PARA RECUPERAÇÃO DE CONTA

- ✓ 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, a vítima 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, o usuário receberá um novo SMS com o novo código de ativação.

QRL JACKING
ESPELHAMENTO INDEVIDO DO WHATSAPP

COMO FUNCIONA O ESPELHAMENTO DO WHATSAPP

Phishing é uma maneira desonesta que cibercriminosos usam para enganar a vitima 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 da vítima, os criminosos criam páginas bem elaboradas de ***phishing***, com ***QR Coding*** do Whatsapp, permitindo que capturem a sessão do aplicativo quando o usuário faz o *login* por meio do Whatsapp Web ou Desktop.

A vítima utilizará normalmente o Whatsapp pelo smartphone, enquanto o criminoso terá acesso ao aplicativo pelo Whatsapp Web, conseguindo acessar as conversas da vítima 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 DO ACESSO A CONTA DO INSTAGRAM

- Caso um usuário tenha perdido acesso ao Instagram, deverá, primeiramente, acessar a conta de e-mail vinculada ao aplicativo e localizar a mensagem, informando a modificação.
- 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.

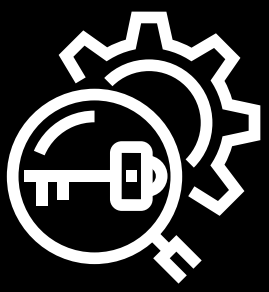
Usar senha distinta para acessar o Instagram e o e-mail vinculado.

OUTROS PROCEDIMENTOS PARA RECUPERAÇÃO DA CONTA DO *INSTAGRAM*

INVASÃO CRIMINOSA

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

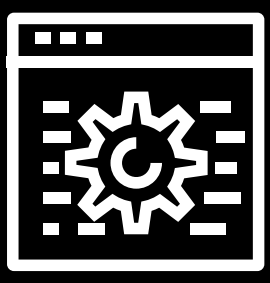
O pedido é feito por ofício, devendo conter um novo e-mail para acesso da vítima.



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

CONCEITO DE *BOLWARE*

É o ***malware*** instalado no computador da vítima para a modificação dos dados de criação e pagamento do boleto bancário.

Quando a vítima 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.

DICAS DE COMO SE PROTEGER DA FRAUDE DE BOLETOS

- 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.

Para melhor compreensão, observe o seguinte exemplo:

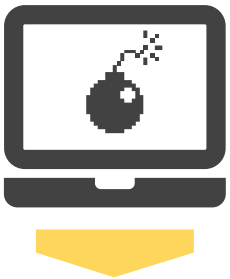
FRAUDE ELETRÔNICA POR RAT BANCÁRIO (REMOTE ACCESS TROJAN)

CONCEITO DE RAT

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

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

Matéria recentemente publicada na internet destaca que pelo menos 20 mil smartphones no Brasil foram infectados por um malware criado para acessar contas bancárias remotamente, por meio de apps dos próprios bancos. *(https://www.mobiletime.com.br/noticias/07/03/2019/malware-brasileiro-disseminado-por-whatsapp-acessa-apps-bancarios/)*.



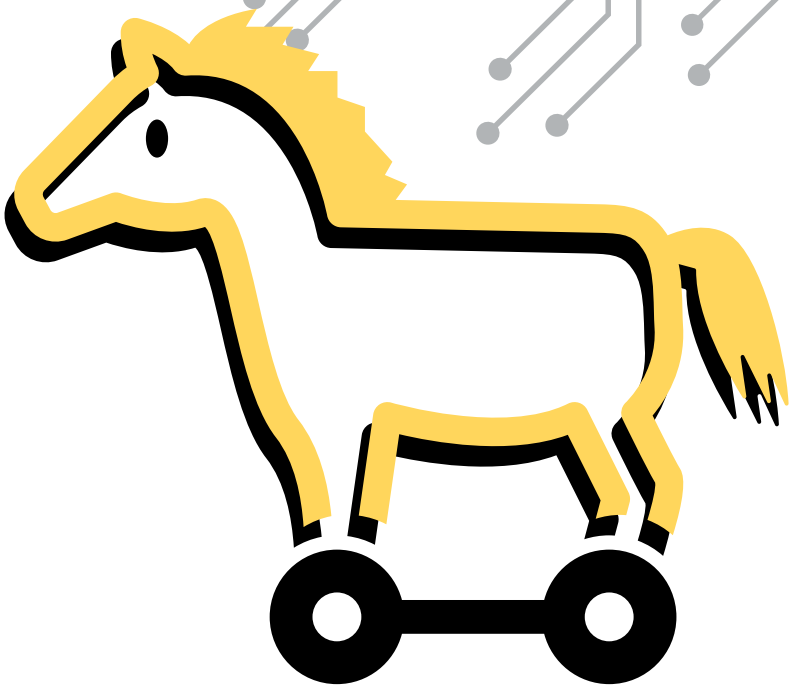
DICAS DE PREVENÇÃO

Manter o antivírus e sistema operacional atualizados.

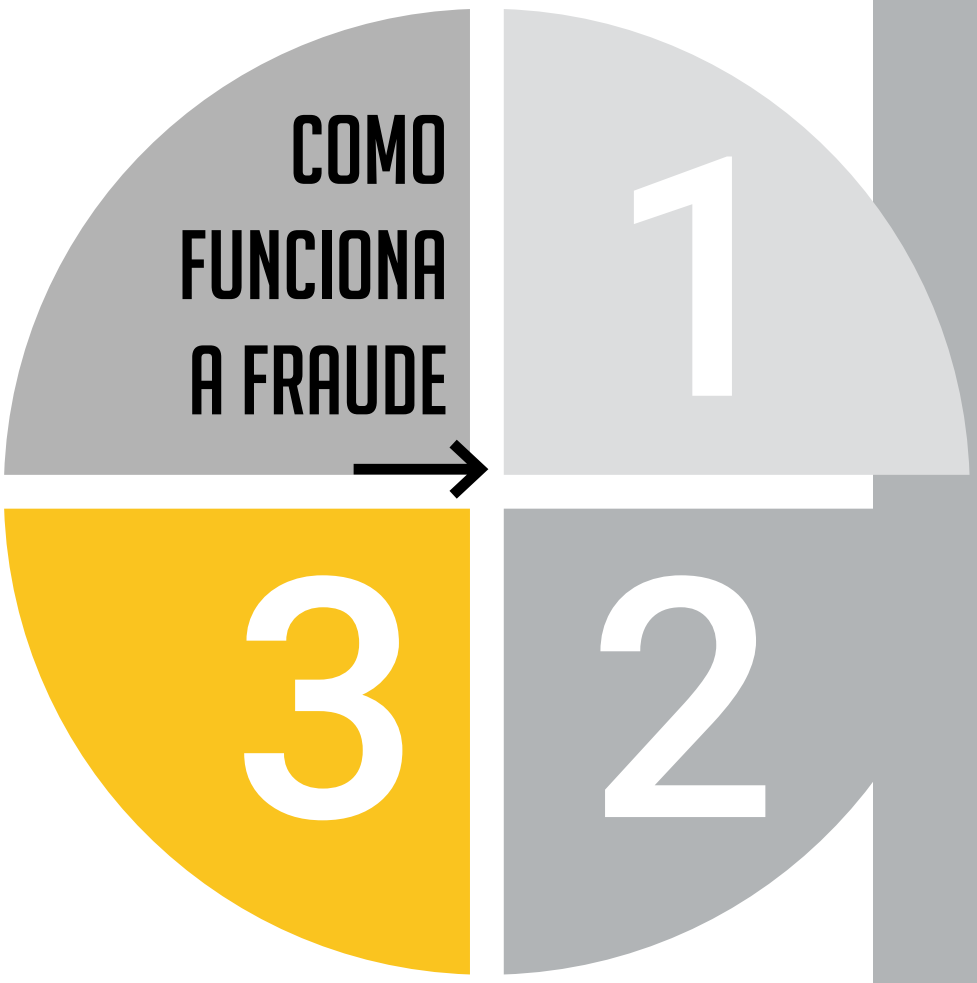
Evite abrir anexos de e-mails de fontes não confiáveis.

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 pelos usuários.

2 ABERTURA PELA VÍTIMA

A vítima, acreditando se tratar de algo de seu interesse, abre e executa o RAT, dando aos criminosos acesso e controle ao seu dispotivo.

3 DESVIO DE DINHEIRO DA CONTA

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

TYPOSQUATTING – "SEQUESTRO" DE URL

CONCEITO DE TYPOSQUATTING

- É normal abrir o navegador e, por algum equívoco, digitar erradamente o nome do domínio que se pretende acessar. Aproveitando-se dessa corriqueira situação, 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.

Veja exemplo de sequestro de URL utilizado para fraude eletrônica:

PRESERVAÇÃO DE EVIDÊNCIA CIBERNÉTICA

MANEIRAS DE GARANTIR A GUARDA DE DADOS PELAS APLICAÇÕES DE INTERNET

ATA NOTARIAL

- É lavrada por tabelião, que deverá registrar os fatos expostos na internet ou em meio digital (mídias sociais, e-mail, whatsapp, etc), conforme previsão do art. 384 do CPC.
- É dotada de fé pública.
- O tabelião não pode emitir opinião, juízo de valor ou conclusão.

CERTIDÃO POLICIAL

- É lavrada por escrivão de polícia, a requerimento da parte, cotendo descrição dos fatos e dados da aplicação de internet, como perfil, página, usuário, ID ou URL.
- O escrivão irá salvaguardar imagens, vídeos e áudios em meio digital.

PRINT SCREEN

- A captura de tela é uma das opções mais utilizadas para salvar um conteúdo da tela de um dispositivo informático. Apesar de guardar alguns elementos, deixa de registrar outros dados relevantes para atribuição de autoria.

OFÍCIO DA AUTORIDADE POLICIAL

- Delegado de polícia requisita a preservação dos registros de acesso, após identificar no documento a URL, perfil, página, conta e-mail ou outro dado relacionado.
- Previsão no art. 15, §2°, do Marco Civil da Internet, e art. 6°, I e III, do CPP.

FACEBOOK RECORDS

- Plataforma de comunicação de preservação de dados do Facebook e do Instagram (www.facebook.com/records).
- Podem solicitar a guarda de dados, por meio da plataforma, a Polícia, o Ministério Público e o Poder Judiciário.

REMOÇÃO DE CONTEÚDO

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

EXCLUSÃO DE CONTÚDO SEM ORDEM JUDICIAL

Em redes sociais e plataformas de conteúdo digital, como Facebook, Twitter **e** Youtube, ***é possível denunciar diretamente o conteúdo postado.***

O usuário 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 (art. 21 do Marco Civil da Internet):

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
>
> Parágrafo único. A notificação prevista no *caput* deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

EXCLUSÃO DE CONTEÚDO SEM ORDEM JUDICIAL

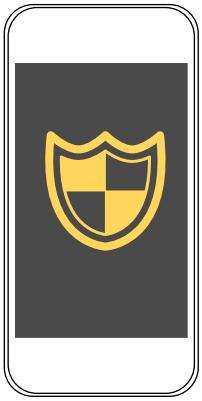
O art. 19 do Marco Civil da Internet dispõe que a exclusão de conteúdo postado na internet, em regra, necessita de ordem judicial.

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.

CONTEÚDO VIRAL NO WHATSAPP

INTERRUPÇÃO DE COMPORTAMENTO 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 DA 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.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRETO, Alessandro Gonçalves. *Cybercards – Meio Cibernético: Orientações Práticas*. 2019.

Fui vítima de um golpe em compra pela web. O que devo fazer? Disponível em: <https://new.safernet.org.br/content/fui-v%C3%ADtima-de-um-golpe-em-compra-pela-web-o-que-devo-fazer>

JORGE, Higor Vinicius Nogueira. *Orientações sobre utilização segura do Whatsapp – Como prevenir a clonagem de Whatsapp e o que fazer se você for vítima*. Versão 2019.1

Proteção contra phishing e golpes. Disponível em: https://new.safernet.org.br/content/prote%C3%A7%C3%A3o-contra-phishing-e-golpes?

Segurança digital. Disponível em: https://new.safernet.org.br/content/seguran%C3%A7a-digital


TJMG