
banco
bmg
Aprenda a se proteger
de crimes cibernéticos

Sumário

WhatsApp

Como os criminosos atuam na clonagem via WhatsApp? 4

Se você caiu no golpe e pretende recuperar sua conta, você deve 5

Dicas para se prevenir 6

Redes Sociais

Hackeamento da conta do Instagram, como agir? 7

Fraudes Financeiras

Alteração de Boleto Bancário 8

Fraude Eletrônicavpor RAT Bancário 10

Conceito Typosquatting (Fraude de sites) 11

O que fazer?

Como proceder se você foi vítima de algum crime? 12

O mundo de hoje é moderno, dinâmico, conectado e com interações em tempo graças à internet. Por um lado, isso facilita nossos relacionamentos, mas por outro, essas interações trazem novos desafios como o de proteger nossos dados de criminosos.

No cenário nacional assistimos às matérias jornalísticas sobre diversos crimes cibernéticos, como conversas interceptadas, clonagem de telefones, fotos e vídeos expostos para milhões de pessoas. **Esses acontecimentos revelam a fragilidade de nossa segurança, não é mesmo?**

Em virtude disso, falar de Segurança Virtual é quase obrigatório.

Nesta cartilha, você vai aprender de forma objetiva, diversas formas de precaução e também o que fazer caso seja vítima de algum golpe.

Vamos lá!

Como os criminosos atuam na clonagem via 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 da vítima, alega ser da empresa de comércio eletrônico e solicita a atualização de seus dados cadastrais.

3. Na ocasião, **pede que seja fornecido a ele, via WhatsApp, o código de 6 (seis) dígitos enviado por SMS pela empresa de comércio eletrônico.**

4. O objetivo **do golpista é acessar o WhatsApp da vítima por meio do número de telefone vinculado à sua conta**, e, para tanto, precisa do código de 6 (seis) dígitos enviado por SMS.

5. A vítima é levada a acreditar que tal código é necessário para realizar a atualização de seu cadastro na empresa de comércio eletrônico e, por isso, fornece os números ao golpista.

6. Após repassar o código recebido por SMS para o golpista, via WhatsApp, **o criminoso conseguirá acessar a conta de WhatsApp da vítima** e, então, solicitará empréstimos aos seus contatos por meio de transferências bancárias.

Se você caiu no golpe e pretende recuperar sua conta, você deve:

- **Registrar Boletim de Ocorrência.**
- Enviar um e-mail para **support@whatsapp.com.**
- No assunto, escrever: **“Perdido/Roubados: Por favor, desative minha conta”.**
- No corpo da mensagem, c**olocar o número do telefone com o código do país e número de DDD.** Ex: +55 33 99999-9999.
- **A empresa WhatsApp irá desativar sua conta,** que, então, poderá ser reativada após 7 (sete) dias.

Como os criminosos atuam na clonagem via WhatsApp?

Phishing é uma maneira desonesta que cibercriminosos usam para **enganar a vítima para que ela revele informações pessoais, tais como senhas de cartão de crédito/débito, CPF e número de contas bancárias.** Eles fazem isso enviando e-mails falsos e/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 Code do WhatsApp,** permitindo que capturem a sessão do aplicativo quando o usuário faz o login por meio do WhatsApp Web ou Desktop. **A vítima cotinuará usando o WhatsApp normalmente pelo seu smartphone, mas o golpista terá acesso ao aplicativo pelo WhatsApp Web falsificado,** conseguindo acessar as conversas da vítima com seus contatos.

Dicas para se prevenir

- Não escanear o **QR Code do celular** em sites desconhecidos.
- Acesse o aplicativo apenas pelo **WhatsApp Web ou na versão Desktop.**
- Evite utilizar o WhatsApp Web em **conexões públicas ou pouco confiáveis.**
- Verifique, com frequência, as sessões ativas do smartphone. Em sistemas 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 direito da tela> WhatsApp Web> Sessões Ativas.**
- Por fim, lembre-se sempre de manter atualizada sua versão do WhatsApp.

Hackeamento da conta do Instagram, como agir?

Caso o 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.

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

- Habilite a verificação em duas etapas.

Outros procedimentos

Invasão criminosa

- Após o registro da ocorrência, a autoridade policial poderá requisitar a **recuperação da conta.**
- O pedido é feito por ofício, e deve conter um novo e-mail para acesso da conta da vítima.

Evento não criminoso

- Denunciar a conta.
- Android: na tela de login, clique em “Obter ajuda para entrar”.
- iOS: na tela login, clique em “Esqueceu a Senha?”

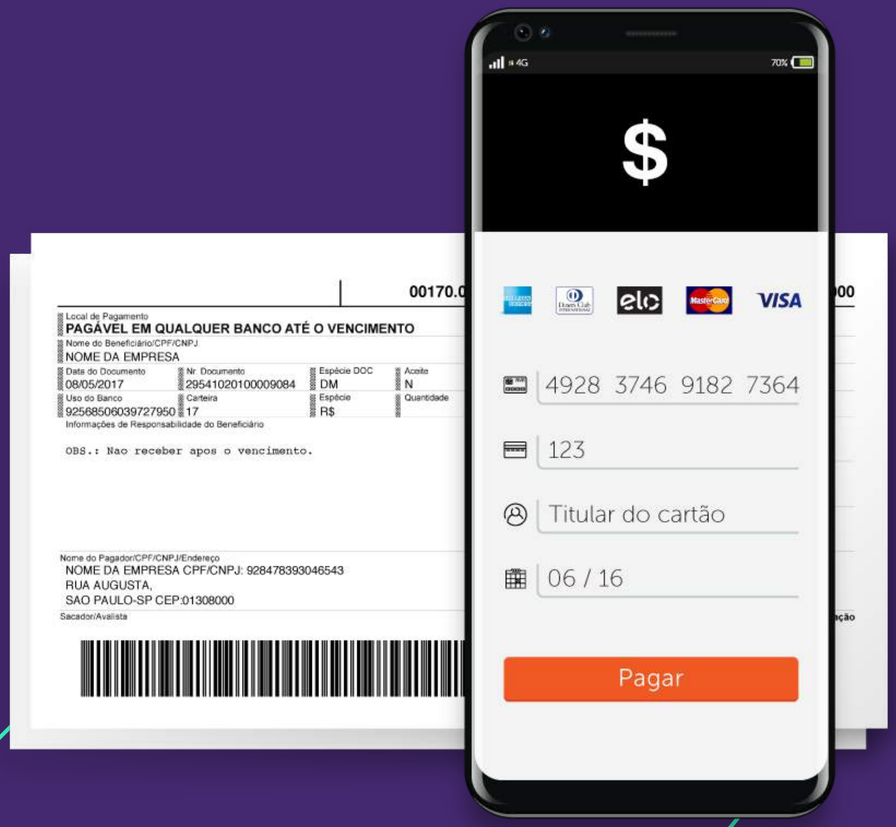
Alteração de Boleto Bancário

Quando a vítima gera o documento para pagamento através de **um computador infectado, o malware altera a linha digitável,** fazendo com que os valores sejam repassados para a conta de terceiros e não para o verdadeiro cedente/ beneficiário.

Dicas para se prevenir

Alguns Cuidados

- Mantenha o **antivírus e o sistema operacional atualizados.**
- **Evite abrir links de terceiros e anexos** de e-mails de fontes desconhecidas.
- O boleto deve ter nome e logotipo do banco emissor coincidentes.
- Dados sobre as instituições financeiras podem ser consultados pelo site Busca da FEBRABAN **(http://www.buscabanco.org.br/).**
- Observe todas as informações do boleto.



- O número do banco e os 3 (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.**
- **Certifique-se da fonte de emissão,** pois a maior parte dos criminosos envia boletos falsos via e-mail e/ou redes sociais. **Se você não solicitou o boleto por email, ligue para o banco e confirme a origem do boleto.**

Para melhor compreensão, observe o seguinte exemplo:

Código do banco

Agência

Valor do documento

bmg 318-2 31890.00502 50500.500900 00010.451896 7 85290000002000

Local de Pagamento
Pagavel em qualquer banco até o vencimento

Vencimento
12/02/2021

Beneficiário
BANCO BMG S/A

CNPJ
61.186.680/0001-74

Agência/ Código Beneficiário
0005 / 050500500-9

Endereço Beneficiário
AV. PRES. JK, 1830 - 10º ANDAR TORRE 1 - ITAIM BIBI - SÃO PAULO - SP

Nosso Número
001/001045189

Data do Documento	Número do Documento	Espécie Doc.	Aceite	Data do Processamento
09/02/2021	0	OU	NAO	09/02/2021

(=) Valor documento **20,00**

Uso do Banco	Carteira	Espécie	Quantidade	Valor
		REAL		x

(-) Desconto/abatimento

Instruções (Todas as informação deste boleto são de exclusiva responsabilidade do beneficiário)

NÃO RECEBER APÓS O VENCIMENTO.
ESTE BOLETO É EXCLUSIVO PARA APENAS UM ÚNICO PAGAMENTO.
SAC 0800 979 90 99 Ouvidoria 0800 723 2044 Deficiente auditivo e/ou de fala: 0800 979 7333

(+) Outras Deduções

(+) Mora/multa

(+) Outros acréscimos

(=) Valor Cobrado **20,00**

Pagador
FERNANDO CESAR GONCALVES DUARTE GUERRA **036.707.116-94**
R TEREZINHA LOPES DE AZEVEDO 183 201
31730-560 - PLANALTO - BELO HORIZONTE - MG

Sacador/Avalista - FERNANDO CESAR GONCALVES DUARTE GUERRA

Autenticação mecânica

Atente-se a falha no código de barras, pois podem utilizar disso para te farçar a digitar um código que irá transferir o valor pago a uma conta não pretendida.

Fraude Eletrônica por RAT Bancário

O RAT (Remote Access Trojan) bancário, ou **“Trojan de Acesso Remoto” é um malware utilizado pelos criminosos para assumir o controle do computador da vítima**, subtrair suas credenciais de acesso ao Internet Banking e, então, desviar valores de suas contas.

Dicas para se prevenir

- Mantenha o **antivírus e o 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.**

Conceito Typosquatting
(Fraude de sites)

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

Em suma, os criminosos normalmente pretendem o seguinte:

a) praticar fraudes eletrônicas (ex.: vender produtos e não realizar a entrega);

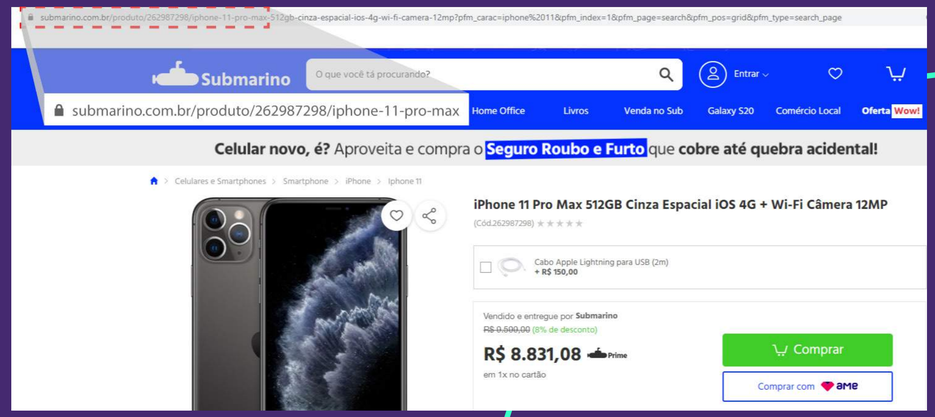
b) vender domínio ou redirecionar tráfego para concorrente;

c) compartilhar fake news;

d) monetizar páginas com publicidade.

Veja o exemplo de sequestro de URL utilizado para fraude eletrônica:

Atente-se para:
- cadeado no site original;
- links suspeitos;
- preços coerentes, ou não, com o mercado.



Como proceder se você foi vítima de algum crime?

O primeiro passo é **fazer uma ocorrência policial** e fornecer algumas informações obrigatórias.

O que preciso informar?

Data, hora e local do último acesso, a conexão de internet utilizada (dados, wi-fi, etc.), conta de e-mail vinculada e, ainda, relatos da conta utilizada pra postagens ou envio de e-mail.

Arquivos suspeitos: **Informe se houve acesso à sites suspeitos,** instalação recente de novos softwares ou cliques em links duvidosos.

Denunciar: **Informe se já efetuou alguma denúncia** sobre a perda de acesso ou hackeamento de sua conta diretamente no provedor de e-mail ou na rede social em questão

Referências

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-comprapela-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

A prevenção é a melhor forma de aproveitar os benefícios da internet.

Esteja sempre atento!

Abraços.

Segurança da Informação

banco bmg