Malware

Segurança de Software

- Essa segurança inclui, principalmente, segurança contra vírus, worm, cavalo de tróia e controle de software instalados – para impedir que nenhum software não autorizado pelo administrador seja instalado nas máquinas de trabalho ou que seja instalado um software pirata.

Segurança de Software

- **Vírus:** Programas maliciosos que se multiplicam contaminando arquivos, registros de inicialização e tabelas de partição dos discos. Para que o vírus seja ativado, é necessário abrir um arquivo contaminado ou inicializar o sistema com um disco contaminado.

- *Solução:* Programas antivírus, detectam e eliminam vírus.

Segurança de Software

- **Cavalos de Tróia (trojans):** São programas maliciosos que geralmente causam o mesmo tipo de problema que os vírus mas não se multiplicam apenas tem alguma função nociva predeterminada.

- *Solução:* Os programas antivírus também combatem os cavalos de Tróia mas para maior proteção é recomendável utilizar um programa específico, o anti trojan que geralmente detecta e remove uma quantidade maior de cavalos de Tróia que os antivírus de uso geral.

Segurança de Software

- **Worms:** São como os vírus mas se multiplicam automaticamente, geralmente exploram falhas de segurança em programas de gerenciamento de e-mails para se auto executarem e se espalharem rapidamente causando sérios prejuízos a nível mundial.

- *Solução:* Programas antivírus e correções de segurança (patches) fornecidos pelos desenvolvedores dos sistemas operacionais e dos programas.

Segurança de Software

- **Spywares :** São um tipo relativamente novo de malware (programa malicioso) utilizados por empresas de marketing para fazer propagandas abusivas e coletar dados sobre os usuários, seus hábitos de navegação, etc. Os spywares são obitidos geralmente através de determinados programas (geralmente os que exibem anúncios comerciais) através de scripts e plugins em páginas de Internet.

- *Solução:* Pogramas anti-spyware que detectam e removem os spywares e alguns também impedem a instalação dos mesmos através de diversos métodos.

Segurança de Software

- Backdoor: Para fazer uma simulação com a realidade, um *backdoor* seria como uma "**entrada secreta"** a uma fortaleza, oculta para a maioria, no entanto, conhecida por poucos que podem aproveitar para entrar sem serem vistos e realizar suas ações. Por sua vez, um trojan seria, tal e como a referência mitológica do nome indica, algo que deixamos acessar a nossa fortaleza e que, uma vez dentro nos causa algum dano.

- **Tipos de *backdoors*? São necesariamente perigosos?**

  O uso de *backdoors* normalmente é integrado aos trojans. Graças a esta usabilidade, um atacante pode conectar-se sempre que quiser aos sistemas infectados, atualizar ou trocar os *malware* instalados para que realizem todo tipo de atividades ou roubar informações sem que o usuário se dê conta, entre outras coisas.

  No entanto, talvez os tipos que mais preocupam são aqueles que permanecem **ocultos a visão** durante longos períodos de tempo e que já vem instalados em alguns sistemas ou aplicativos. Isso permite aos cibercriminosos um grande poder sobre os sistemas afetados, permitindo o **controle** sobre os mesmos.

Segurança de Software

- Software instalado: é fundamental que a empresa tenha controle de todos os softwares instalados em seu parque de máquinas. Cada estação deve ser auditada periódicamente.
- O software é considerado seguro quando faz exatamente o que se espera dele, nem mais nem menos. Isto é um software livre de bugs.
- Bug é um erro no código do programa que faz com que instruções erradas sejam executadas, causando danos.
- Alguns bug podem ser projetados e são chamados de Backdoors, ou seja, uma ameaça programada que permite acesso não autorizado ao sistema ou aplicativo sem ter que passar pelo processo normal de autenticação.

Antimalwares e Firewalls

Antimalwares

1. Kaspersky Total Security
2. Bitdefender Internet Security
3. Avira Internet Security
4. Panda Dome Advanced
5. Norton 360 Deluxe
6. Bitdefender Antivírus Free Edition
7. Kaspersky Security Cloud Free
8. Panda Free Antivírus
9. Avira Segurança Gratuita
10. Avast Free Antivírus

Firewalls

1. Comodo Firewall
2. Zone Alarm Free Firewall
3. TinyWall
4. Firewall App Blocker

Heurística

A Verificação Heurística é a capacidade que um antivírus possui de detectar um malware, sem possuir uma vacina específica para ele, ou seja, a idéia da heurística é a de antecipar a descoberta de um malware. Existem softwares anti-spam que trabalham com a mesma filosofia. O grande problema deste tipo de método de detecção está na possibilidade de se encontrar um número muito alto de falsos positivos. Os falsos positivos são os arquivos que possuem algumas características que podem parecer com malwares, mas não os são.

Além disso, esta técnica também possui uma verificação mais lenta, pois o processo de procurar arquivos que possuam determinadas características é diferente de se procurar malwares já reconhecidos.

Esta técnica também não identificará novos malwares que possuam características diferentes dos malwares já reconhecidos, pois a heurística esta preparada para detectar características comuns a outros malwares.

Engenharia Social

Engenharia social é o termo utilizado para definir o conjunto de métodos e técnicas (computacionais e psicológicas) empregado por golpistas com o intuito de manipular e persuadir determinada pessoa a revelar **dados pessoais ou informações corporativas,** ou comprometer sistemas computacionais para atingir tal fim.

Esse tipo de golpe pode ser executado com a obtenção de informações pessoais mediante simples pesquisa nas redes sociais da vítima ou com a utilização de meios tecnológicos, como malwares.

Dados pessoais e informações coorporativas são ativos de grande importância não só no mundo empresarial, mas para sociedade em geral.

O desenvolvimento tecnológico proporcionou inúmeros benefícios para a sociedade. Porém, com a evolução das novas tecnologias, cresceram exponencialmente as vulnerabilidades de sistemas. Hackers e golpistas exploram essas falhas por meio de aplicação de determinadas técnicas, que, somadas ao poder de persuasão, se transformam em oportunidades para a prática de crimes, causando expressivos prejuízos às vítimas e às empresas.

Podemos definir engenheiro social como aquele que – valendo-se de influência e persuasão, de técnicas psicológicas de convencimento ou de meios tecnológicos – consegue facilmente enganar e manipular as vítimas para que revelem ou concedam acesso a dados pessoais ou informações sigilosas, o que resultará na aplicação de diversos golpes, visando obter benefícios econômicos ou praticar fraudes contra terceiros.

Conhecer, ficar atento ao modo de execução e tentar mitigar possíveis vulnerabilidades são, sem dúvida, os meios mais eficazes de impedir a eficiência do golpe.

Engenharia Social

O engenheiro social é perspicaz e habilidoso. Ele coloca em prática o golpe a partir de certos descuidos e, muitas vezes, a partir da ingenuidade da vítima, seja pela exposição excessiva de hábitos pessoais em redes sociais, seja pela divulgação a terceiros de senhas, tokens ou quaisquer outras informações sigilosas.

A prática de engenharia social no ambiente empresarial também é comum e recorrente. Todo ambiente de trabalho dispõe de dados confidenciais e sensíveis, que, em muitas situações, não estão devidamente protegidos.

Documentos esquecidos em impressoras ou copiadoras; papéis reutilizáveis de relatórios e atas de reuniões, contendo assinaturas, números de telefones, e-mails, endereços, agendas, demonstrativos financeiros; crachás expostos fora do ambiente da empresa; catracas sem controle de acesso, muitas vezes, são suficientes para "quebrar" todo o sistema de segurança de uma empresa.

É necessário ficar atento a abordagens em telefonemas. Muitas vezes, as ligações são feitas por indivíduos que se apresentam como conhecidos ou que simulam o contato em nome de instituições reconhecidas no mercado, como seu banco de confiança ou a rede de supermercados que você faz compras habitualmente. Solicitam dados, como senha, login, token, número do CPF, filiação ou outras informações. Em outros tipos de abordagem, pedem endereço de e-mail para envio de anexos, que podem simplesmente, sem que você perceba, abrir a porta para o engenheiro social acessar seu computador ou seu celular.

Engenharia Social

SITES FALSOS

Uma forma altamente eficaz de execução da engenharia social é a criação de sites fraudulentos, apresentados às vítimas basicamente em dois formatos:

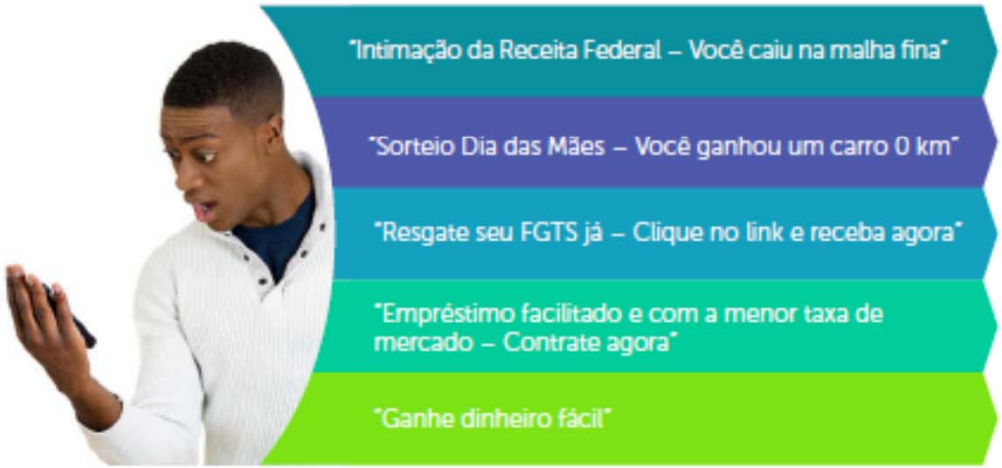
1. Imitação de sites de grandes instituições, que visam induzir a vítima a acreditar que é confiável e legítimo;

2. Sites com conteúdo atrativo para que a vítima seja persuadida a informar dados pessoais para fins cadastrais ou mediante oferecimento de descontos e cupons.

E-MAILS (SPAMS)

Método que consiste no envio de e-mails, que, aparentemente, são originados de fontes confiáveis. Esses e-mails têm como objetivo obter dados pessoais ou informações sensíveis mediante apresentação de conteúdo atrativo que desperte na vítima o interesse em clicar em um link para direcionamento ao site falso. Esse tipo de e-mail também pode conter arquivos maliciosos que infectam celulares, tablets ou computadores.

Veja alguns exemplos de títulos mais comuns utilizados para prática de engenharia social.



REDES SOCIAIS

(Facebook, Instagram, LinkedIn, Twitter, Snapchat)

Com o aumento significativo do número de usuários de redes sociais, golpistas encontraram uma maneira fácil e eficaz de obter informações diversas sobre possíveis vítimas. Com uma simples pesquisa nas redes sociais, é possível traçar os perfis pessoal, profissional e comportamental das vítimas. As publicações que não possuem controle de exibição a terceiros ficam disponíveis para visualização de qualquer usuário e podem ser uma ferramenta muito útil para aplicação de golpes, pois o engenheiro social conhecerá um pouco sobre você.

APLICATIVOS DE COMUNICAÇÃO INSTANTÂNEA

(WhatsApp, Viber, Skype, Facebook Messenger, Telegram)

São responsáveis por possibilitar o fluxo imediato de imenso volume de informações, tais como fotos, vídeos, notícias, documentos e links. A disseminação de links e de arquivos maliciosos por meio de aplicativos de comunicação instantânea é uma técnica muito eficaz utilizada por golpistas. Por isso, fique atento se os conteúdos e links que você recebe são de contatos conhecidos e de confiança, pois essa ferramenta pode ser utilizada pelo engenheiro social para abordagem e aplicação de golpes.

Phishing

O que é phishing

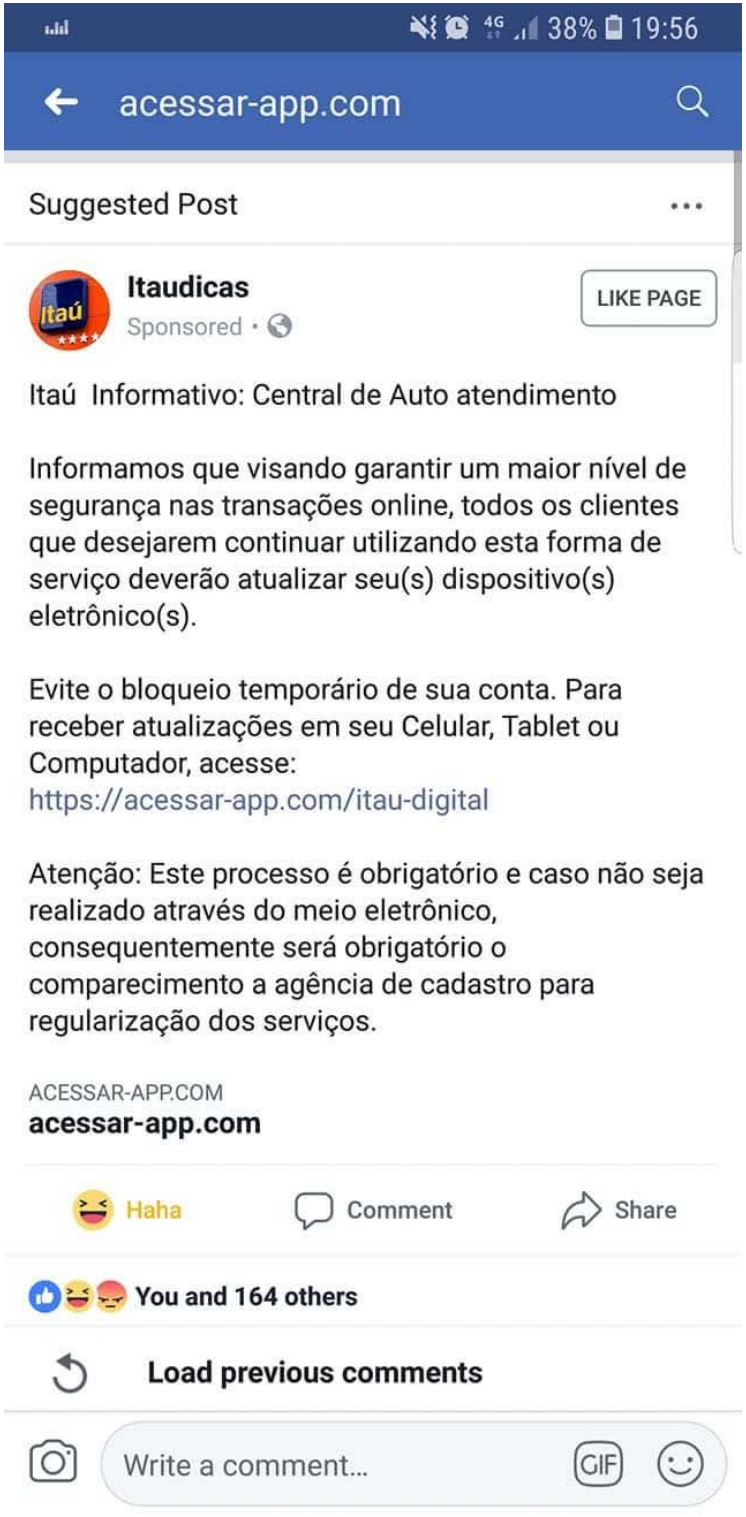
Phishing é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

De onde vem o phishing

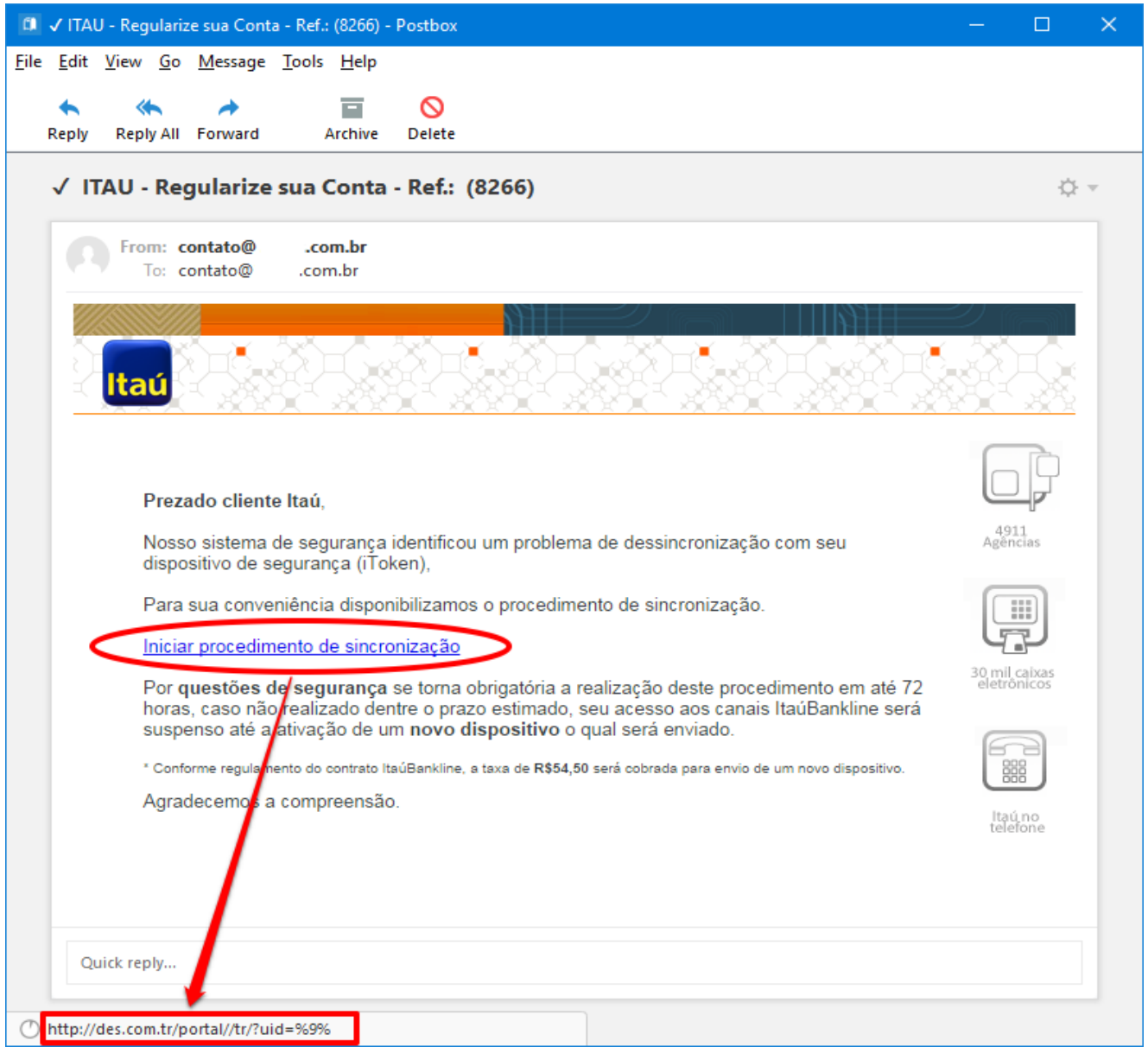
Mensagens de Phishing parecem ser enviados por organizações legítimas como PayPal, UPS, uma agência do governo ou seu banco; entretanto, elas são em fato falsas mensagens. Os e-mails pedem de forma educada por atualizações, validação ou confirmação de informações da sua conta, sempre dizendo que houve algum problema. Você é então redirecionado a um site falso e enganado a apresentar informações sobre a sua conta, que podem resultar em roubos de identidade.

Como reconhecer phishing

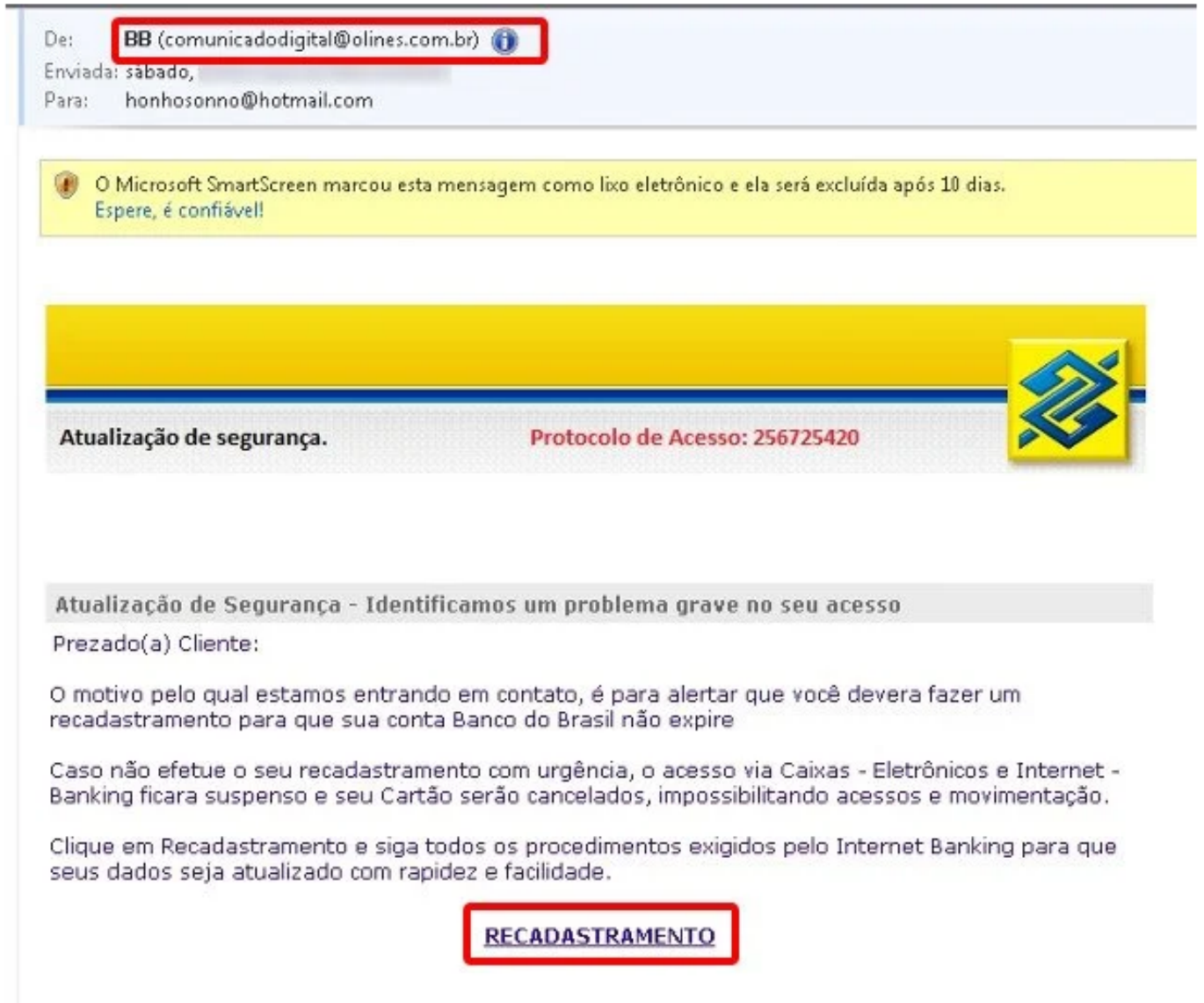
Você recebe mensagens pedindo para você revelar informações pessoais, geralmente via e-mail ou website.



Phishing


✓ ITAU - Regularize sua Conta - Ref.: (8266) - Postbox
File Edit View Go Message Tools Help
Reply Reply All Forward Archive Delete
✓ ITAU - Regularize sua Conta - Ref.: (8266)
From: contato@ .com.br
To: contato@ .com.br
Itaú
Prezado cliente Itaú,
Nosso sistema de segurança identificou um problema de dessincronização com seu dispositivo de segurança (iToken),
Para sua conveniência disponibilizamos o procedimento de sincronização.
Iniciar procedimento de sincronização
Por questões de segurança se torna obrigatória a realização deste procedimento em até 72 horas, caso não realizado dentre o prazo estimado, seu acesso aos canais ItaúBankline será suspenso até a ativação de um novo dispositivo o qual será enviado.
* Conforme regulamento do contrato ItaúBankline, a taxa de R$54,50 será cobrada para envio de um novo dispositivo.
Agradecemos a compreensão.
4911 Agências
30 mil caixas eletrônicos
Itaú no telefone
Quick reply...
http://des.com.tr/portal//tr/?uid=%9%

Phishing



De: BB (comunicadodigital@olines.com.br)
Enviada: sábado,
Para: honhosonno@hotmail.com

O Microsoft SmartScreen marcou esta mensagem como lixo eletrônico e ela será excluída após 10 dias.
Espere, é confiável!

Atualização de segurança. **Protocolo de Acesso: 256725420**

Atualização de Segurança - Identificamos um problema grave no seu acesso

Prezado(a) Cliente:

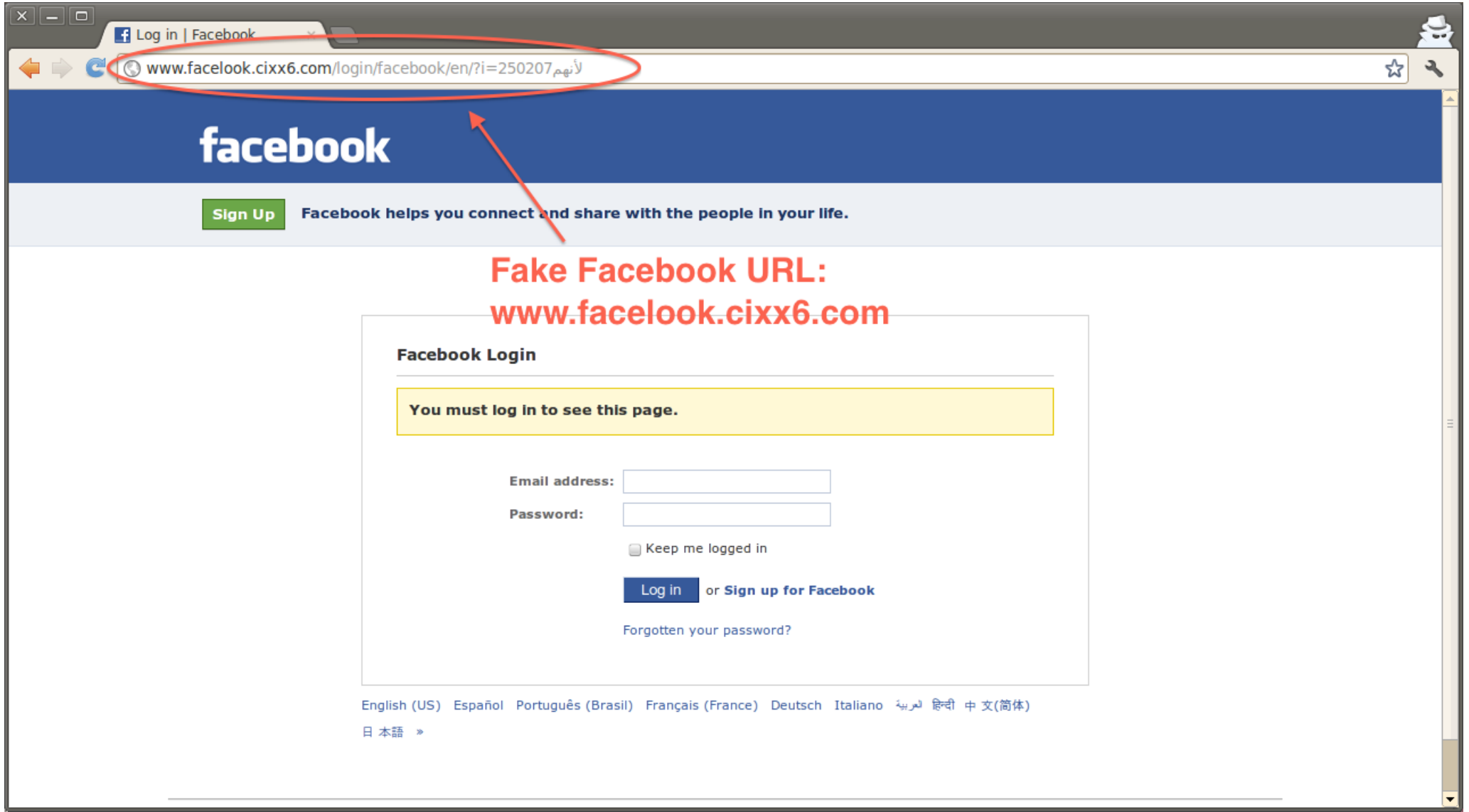
O motivo pelo qual estamos entrando em contato, é para alertar que você devera fazer um recadastramento para que sua conta Banco do Brasil não expire

Caso não efetue o seu recadastramento com urgência, o acesso via Caixas - Eletrônicos e Internet - Banking ficara suspenso e seu Cartão serão cancelados, impossibilitando acessos e movimentação.

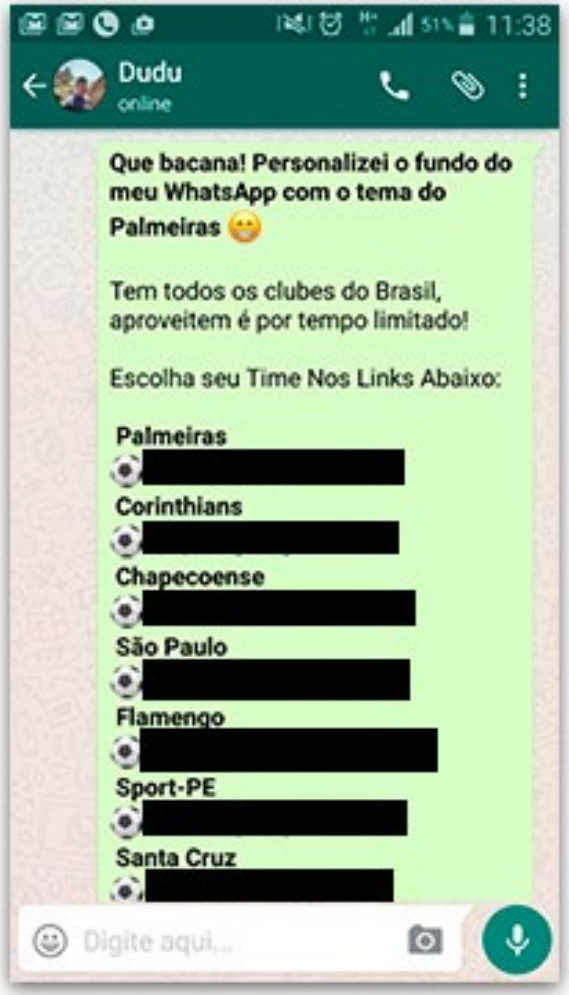
Clique em Recadastramento e siga todos os procedimentos exigidos pelo Internet Banking para que seus dados seja atualizado com rapidez e facilidade.

RECADASTRAMENTO

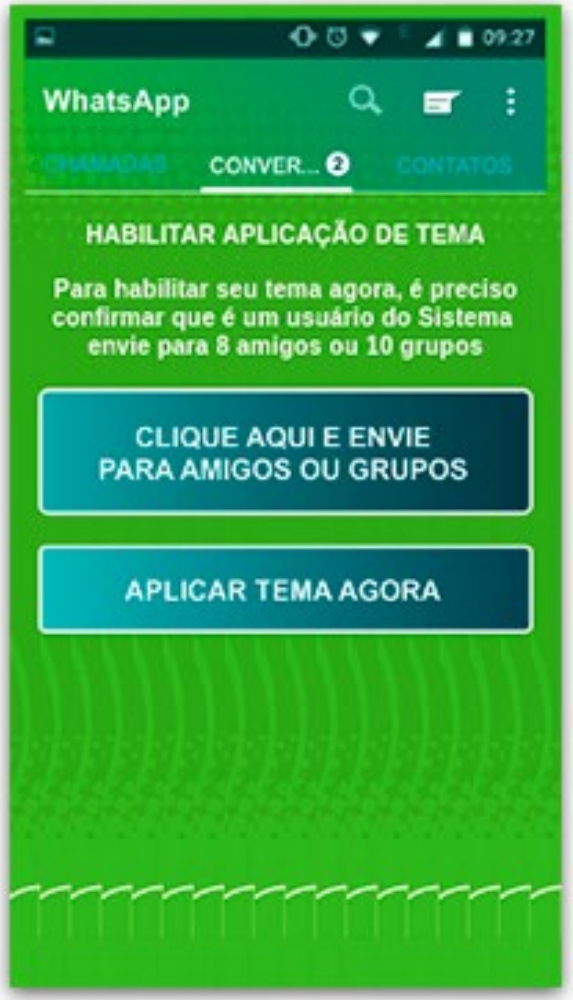
Phishing


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207لأنهم
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Fake Facebook URL:
www.facelook.cixx6.com
Facebook Login
You must log in to see this page.
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語 »

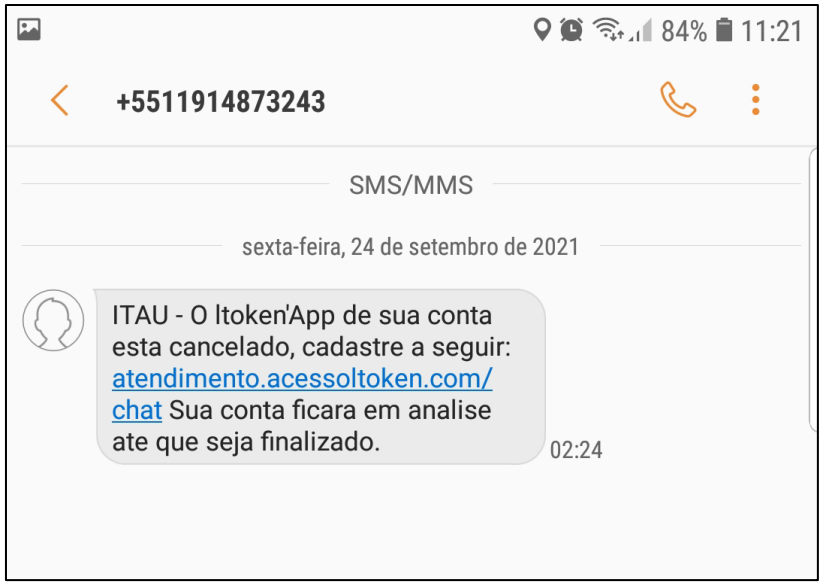
Phishing

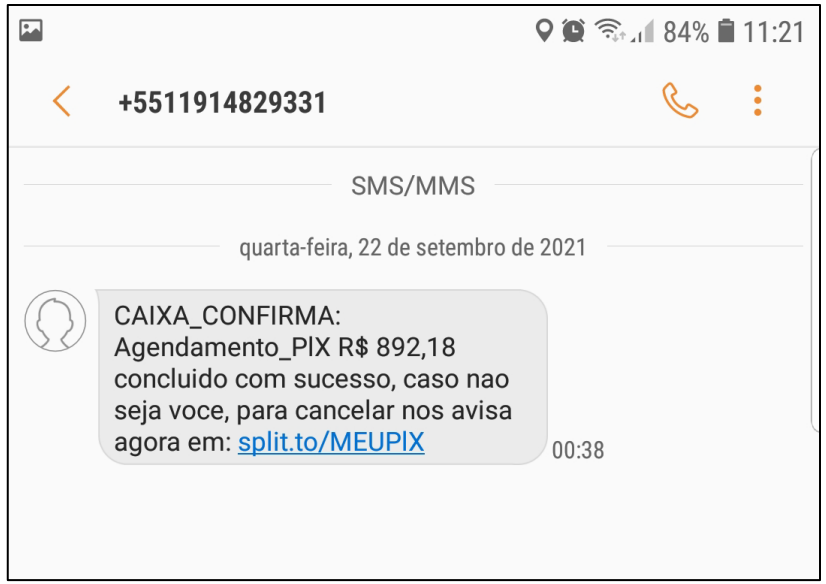

11:38
Dudu
online
Que bacana! Personalizei o fundo do meu WhatsApp com o tema do Palmeiras
Tem todos os clubes do Brasil, aproveitem é por tempo limitado!
Escolha seu Time Nos Links Abaixo:
Palmeiras
Corinthians
Chapecoense
São Paulo
Flamengo
Sport-PE
Santa Cruz
Digite aqui...

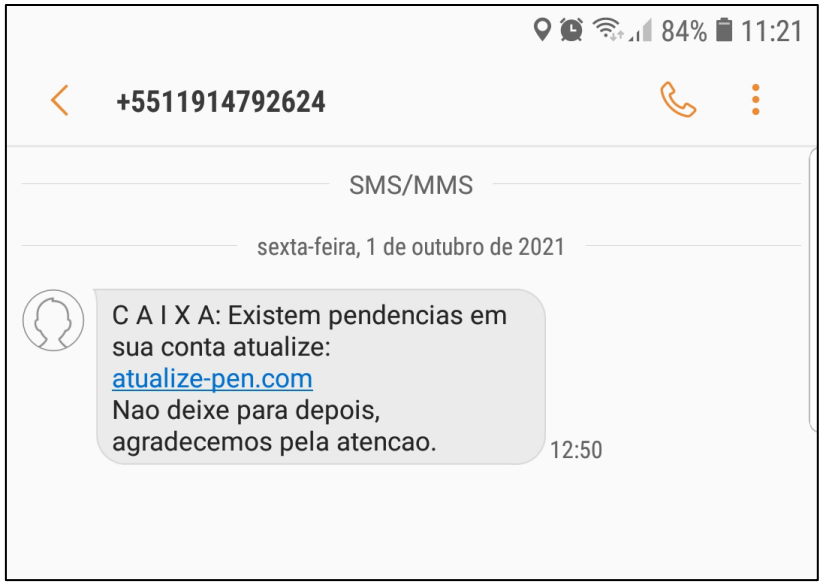

WhatZap TIME
SEJA BEM VINDO!
Agora você pode personalizar o seu WhtasApp com o tema do seu time FAVORITO
ATUALIZE SEU APLICATIVO AGORA!
Seu nome aqui...
Botafogo
HABILITAR TEMA >>>
Disponível para iOS, Android e Windows Phone


09:27
WhatsApp
CONVER...
HABILITAR APLICAÇÃO DE TEMA
Para habilitar seu tema agora, é preciso confirmar que é um usuário do Sistema envie para 8 amigos ou 10 grupos
CLIQUE AQUI E ENVIE PARA AMIGOS OU GRUPOS
APLICAR TEMA AGORA

Phishing


84% 11:21
+5511914873243
SMS/MMS
sexta-feira, 24 de setembro de 2021
ITAU - O ltoken'App de sua conta esta cancelado, cadastre a seguir: atendimento.acessoltoken.com/chat Sua conta ficara em analise ate que seja finalizado.
02:24


84% 11:21
+5511914829331
SMS/MMS
quarta-feira, 22 de setembro de 2021
CAIXA_CONFIRMA: Agendamento_PIX R$ 892,18 concluido com sucesso, caso nao seja voce, para cancelar nos avisa agora em: split.to/MEUPIX
00:38


84% 11:21
+5511914792624
SMS/MMS
sexta-feira, 1 de outubro de 2021
C A I X A: Existem pendencias em sua conta atualize: atualize-pen.com
Nao deixe para depois, agradecemos pela atencao.
12:50

Ransomware

Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

O pagamento do resgate geralmente é feito via bitcoins.

Como ocorre a infecção?

O ransomware pode se propagar de diversas formas, embora as mais comuns sejam:

- através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link;
- explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Quais tipos de ransomware existem?

Existem dois tipos de ransomware:

- Ransomware Locker: impede que você acesse o equipamento infectado.
- Ransomware Crypto: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

Além de infectar o equipamento o ransomware também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também.

Como devo me proteger de ransomware?

Para se proteger de ransomware você deve tomar os mesmos cuidados que toma para evitar os outros códigos maliciosos, como:

- manter o sistema operacional e os programas instalados com todas as atualizações aplicadas;
- ter um antivírus instalado;
- ser cuidadoso ao clicar em links ou abrir arquivos.

Fazer backups regularmente também é essencial para proteger os seus dados pois, se seu equipamento for infectado, a única garantia de que você conseguirá acessá-los novamente é possuir backups atualizados. O pagamento do resgate não garante que você conseguirá restabelecer o acesso aos dados.