Phishing

Prof. Emerson Rocha

O que é Phishing?

Phishing é um tipo de ataque cibernético que usa e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar as pessoas a compartilhar dados confidenciais, baixar malware ou se expor a crimes cibernéticos de outras formas.

É uma forma de engenharia social. Ao contrário de outros ataques cibernéticos, que têm como alvo direto redes e recursos, os ataques de engenharia social usam erros humanos, histórias falsas e táticas de pressão para manipular as vítimas e causar danos involuntários a si mesmas ou a suas organizações.

O que é Engenharia Social?

A engenharia social é uma maneira de manipular as vítimas para **conseguir** informações pessoais com o fim de realizar um ataque que pode comprometer a segurança pessoal ou a segurança de uma rede corporativa.

O que é uma violação de dados?

Uma violação de dados é qualquer incidente de segurança no qual partes não autorizadas obtêm acesso a dados sensíveis ou informações confidenciais, incluindo dados pessoais (números de Segurança Social, números de contas bancárias, informações de saúde) ou dados corporativos (dados de clientes, propriedade intelectual, informações financeiras).

O que é um Ataque Cibernético?

Um ataque cibernético é qualquer esforço intencional para roubar, expor, alterar, desativar ou destruir dados, aplicativos ou outros ativos por meio de acesso não autorizado a uma rede, sistema de computador ou dispositivo digital.

O que é Malware?

Software malicioso, ou malware, é qualquer código de software ou programa de computador, incluindo ransomware, cavalos de Troia e spyware, escrito intencionalmente para prejudicar os sistemas de computador ou seus usuários.

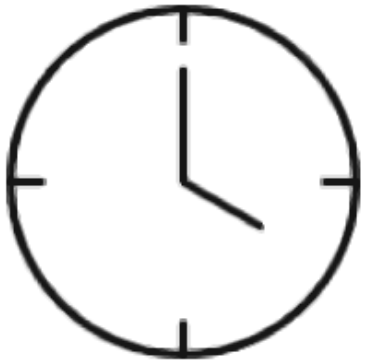
O que é Pretexting?

Pretexting é o uso de uma história fabricada, ou pretexto, para ganhar a confiança de uma vítima e enganá-la ou manipulá-la para compartilhar informações confidenciais, baixar malware, enviar dinheiro para criminosos ou prejudicar a si mesma ou à organização para a qual trabalha.

Quais são os sinais de um ataque de phishing

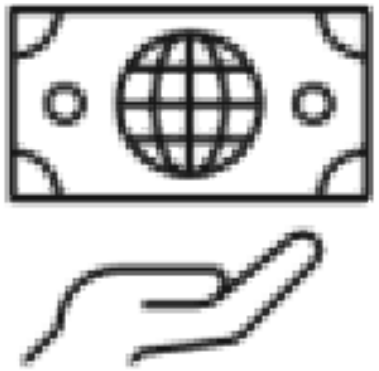
1. **Emoções fortes e táticas de pressão.**

Os golpes de phishing tentam fazer com que as vítimas sintam um senso de urgência para que elas ajam rapidamente sem pensar. Os golpistas costumam fazer isso invocando emoções fortes, como medo, ganância e curiosidade. Podem impor prazos e ameaçar consequências irrealistas, como a prisão.



- "Há um problema com sua conta ou informações financeiras. Você deve atualizá-la imediatamente para evitar a perda de acesso."
- "Detectamos atividades ilegais. Pague essa multa agora, ou então você será preso."
- "Você ganhou um presente, mas deve resgatá-lo agora mesmo."
- "Esta fatura está vencida. Você deve pagá-la imediatamente, ou nós encerraremos seu serviço. "
- "Temos uma excelente oportunidade de investimento para você. Deposite dinheiro agora e podemos garantir retornos incríveis."

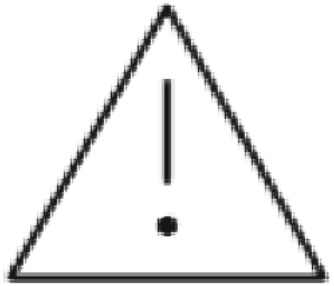
2. **Solicitações de dinheiro ou informações confidenciais**



Os golpes de phishing normalmente pedem uma de duas coisas: dinheiro ou dados.
Solicitações não solicitadas ou inesperadas de pagamento ou informações pessoais podem ser sinais de ataques de phishing.

Os golpistas disfarçam suas solicitações de dinheiro como faturas vencidas, multas ou taxas de serviços. Eles disfarçam as solicitações de informações como avisos para atualizar informações de pagamento ou de conta ou redefinir uma senha.

3. **Erros de ortografia e gramática**

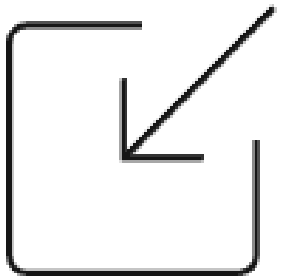


Muitas gangues de phishing operam internacionalmente, o que significa que muitas vezes escrevem mensagens de phishing em idiomas que não falam fluentemente. Portanto, muitas tentativas de phishing contêm erros gramaticais e inconsistências.

4. **Mensagens genéricas**

As mensagens de marcas legítimas geralmente contêm detalhes específicos. Eles podem se dirigir aos clientes pelo nome, fazer referência a números de pedidos específicos ou explicar com precisão qual é o problema. Uma mensagem vaga como "Há um problema com sua conta" sem mais detalhes é um sinal de alerta.

5. **URLs e endereços de e-mail falsos**



Os golpistas geralmente usam URLs e endereços de e-mail que parecem legítimos à primeira vista. Por exemplo, um e-mail de "admin@rnicrosoft.com" pode parecer seguro, mas é preciso verificar novamente. O "m" em "Microsoft" é na verdade um "r" e um "n.“

Outra tática comum é usar um URL como "bankingapp.scamsite.com".

Um usuário pode pensar que isso se vincula a bankingapp.com, mas na verdade aponta para um subdomínio de scamsite.com.

Os hackers também podem usar serviços de encurtamento de links para disfarçar URLs maliciosos.

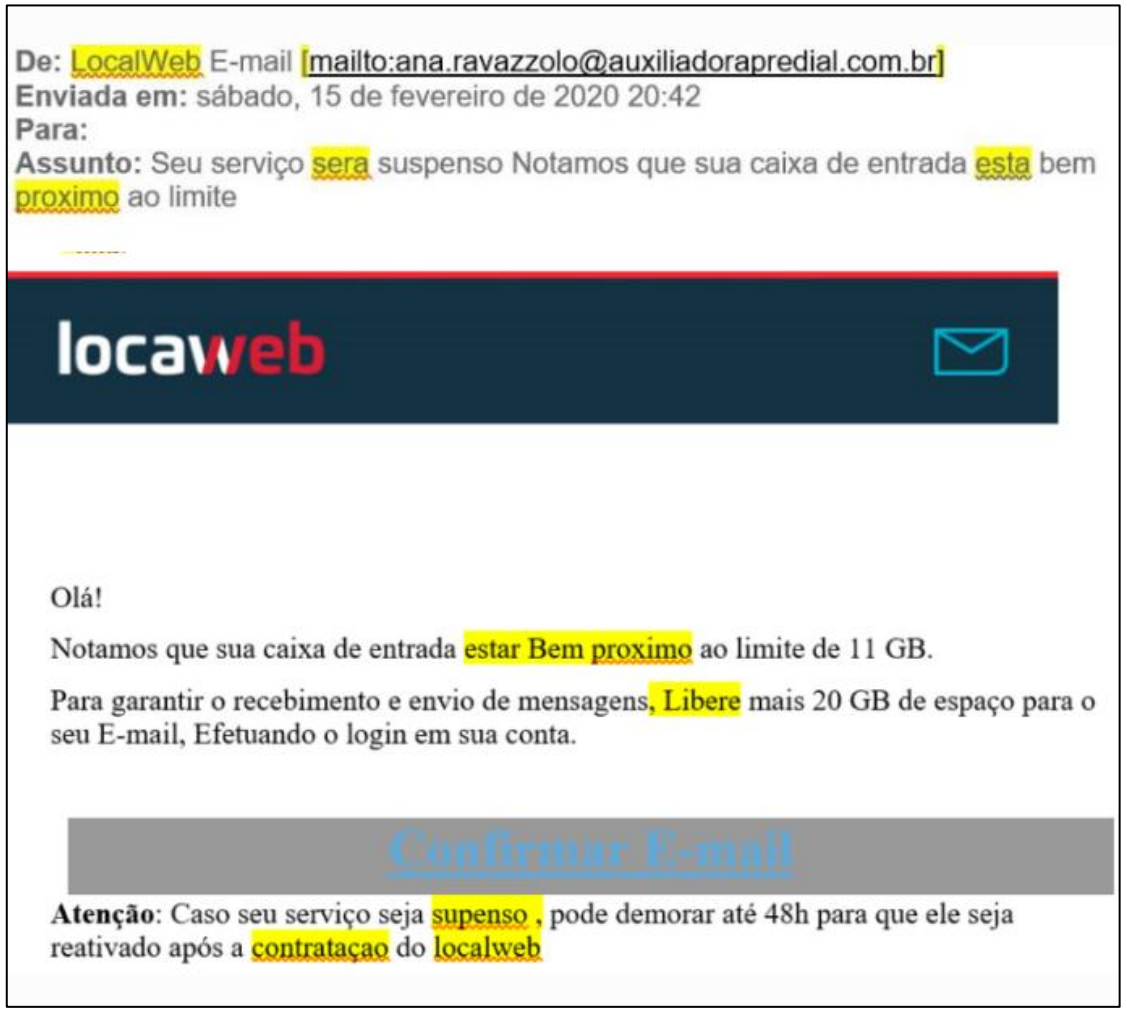
6. **Outros sinais**

Os golpistas podem enviar arquivos e anexos que o alvo não solicitou e não espera.

Eles podem usar imagens de texto em vez de texto real em mensagens e páginas da web para evitar filtros de spam.

Exemplo

Segue abaixo um caso real de tentativa de phishing em um cliente nosso. Reparem nos pontos em destaque amarelo:



De: LocalWeb E-mail [mailto:ana.ravazzolo@auxiliadorapredial.com.br]
Enviada em: sábado, 15 de fevereiro de 2020 20:42
Para:
Assunto: Seu serviço sera suspenso Notamos que sua caixa de entrada esta bem proximo ao limite

locaweb

Olá!

Notamos que sua caixa de entrada estar Bem proximo ao limite de 11 GB.

Para garantir o recebimento e envio de mensagens, Libere mais 20 GB de espaço para o seu E-mail, Efetuando o login em sua conta.

Confirmar E-mail

Atenção: Caso seu serviço seja supenso , pode demorar até 48h para que ele seja reativado após a contrataçao do localweb

- Verifique que no e-mail recebido contém diversos erros ortográficos;

- O e-mail do remetente não é legitimo contendo um domínio que não pertence a Locaweb;

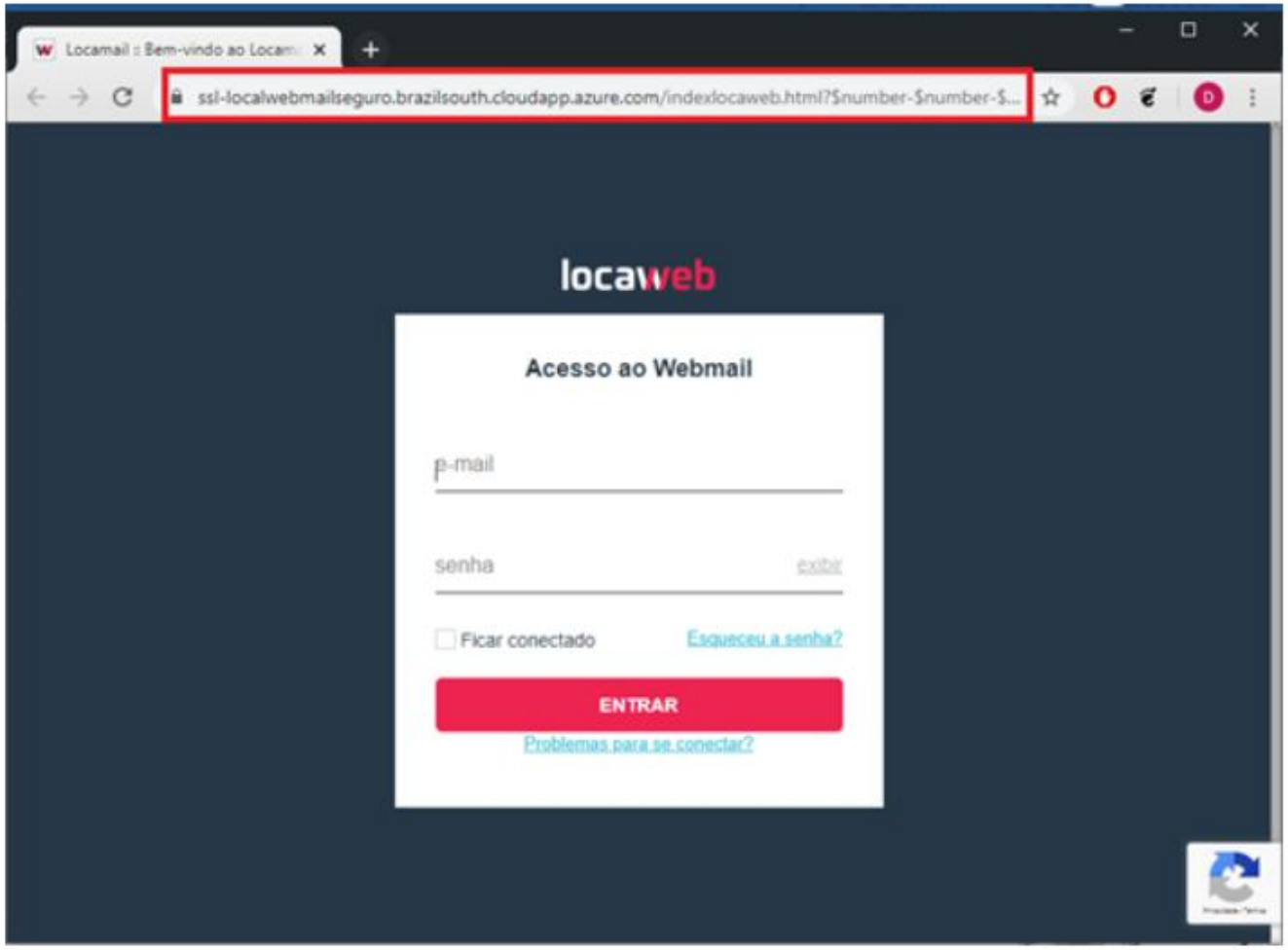
- O e-mail se dirige à pessoa de forma vaga com “Olá!”;

- Ao passar o mouse em cima do link **“Confirmar E-mail”** ele mostra uma página muito suspeita que não é da Locaweb;

- Ele transmite uma certa urgência, informando que se for suspenso ficará por 48 horas sem o serviço;

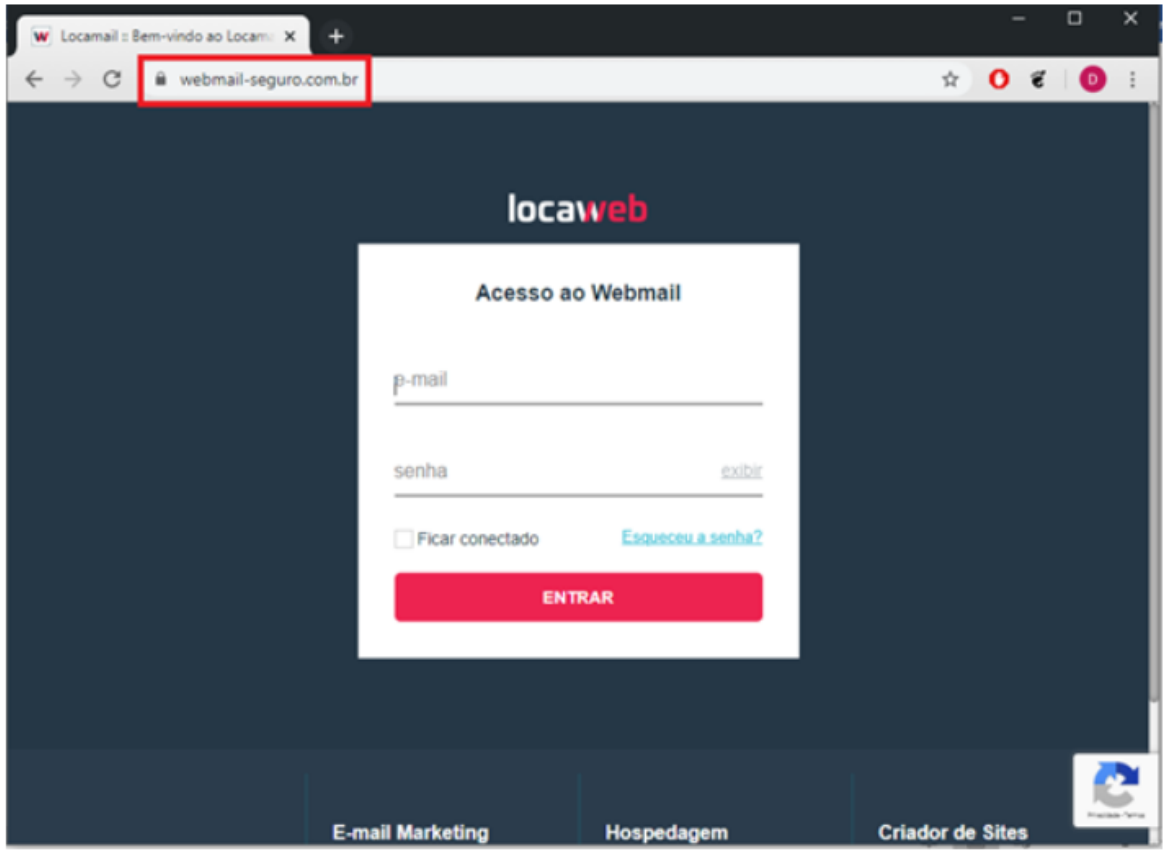
- Em nenhuma parte do e-mail tem o contato da Locaweb.

O link para qual é direcionado no e-mail, é a pagina abaixo. Note que ela é praticamente idêntica a página original, porém como podemos perceber na URL, o endereço não pertence a Locaweb e é bem suspeito:



Se digitar o e-mail e senha, eles são capturados e logo após isso é direcionado para a página original da Locaweb onde muitas vezes a vítima acaba nem percebendo que teve seus dados capturados.

Essa é pagina legitima da Locaweb, note como a URL é diferente:



Referência

https://www.ibm.com/br-pt/topics/phishing

https://ravel.com.br/blog/o-que-e-phishing/

https://www.ibm.com/br-pt/topics/social-engineering

https://www.ibm.com/br-pt/topics/data-breach

https://www.ibm.com/br-pt/topics/cyber-attack

https://www.ibm.com/br-pt/topics/pretexting

https://www.ibm.com/br-pt/topics/malware

https://ravel.com.br/blog/o-que-e-phishing/