Princípios de Segurança da Informação

Engenharia Social

Entenda o que é Engenharia Social e aprenda a se proteger

btg pactual

Por que estar atento à segurança?

As atividades que costumávamos fazer no “mundo físico” agora podem ser facilmente realizadas no mundo virtual.

Isso dá algumas vantagens aos criminosos, pois eles estão pouco expostos à ações policiais (que dependem de muita investigação) e tem uma superfície de ataque muito grande, que é a internet.

Especialista avisa: ataques cibernéticos serão ainda mais comuns em 2021

Notícia do Canaltech em 20 de Dezembro de 2020

Deixamos nossos dados pessoais e bancários, fotos e contatos em diversos sites e redes sociais. Não podemos confiar que todas as comunicações nesse meio serão legítimas.

Além disso, precisamos utilizar a tecnologia a nosso favor, sabendo configurar nossas contas de e-mail e aplicativos da maneira mais segura possível.

Muitas vezes, sabendo como entrar em contato com a vítima e muitas vezes sabendo parte da vida dela, um atacante envia mensagens ou faz ligações forjando situações para tirar alguma vantagem.

Chamamos essa prática de **Engenharia Social**.

O que é Engenharia Social?

No contexto de segurança da informação, são técnicas empregadas por criminosos para induzir a vítima a tomar uma ação, como informar dados, clicar em links, realizar transferências de valores, entre outros.

Quais são os principais golpes que envolvem engenharia social?

- E-mails falsos (phishing). Envio de e-mails falsos genéricos ou direcionados a uma pessoa ou grupo específico.

- BEC (Business E-mail Compromise): esse golpe ocorre por e-mail quando uma das partes é comprometida. Com acesso aos e-mails trocados, o fraudador inicia pedidos de transferência de valores, por exemplo.

- Golpes do WhatsApp: fraudadores se passando por você e entrando em contato com outras pessoas ou mesmo "sequestrando" a sua conta do aplicativo.

Muitas dessas tentativas de golpes vão tentar manipular os sentimentos da vítima, com mensagens que demandam ação urgente, que envolvem relações pessoais ou questões financeiras.

btg pactual

Phishing

Phishing é quando o criminoso envia mensagens aparentemente reais a uma vítima, aguardando que ela tome determinada ação. Hoje a principal porta de entrada de hackers em uma empresa é o phishing. Também é uma maneira fácil de conseguir credenciais válidas de pessoas comuns.

O Brasil lidera o ranking mundial no recebimento de phishings no formato de e-mails falsos já há alguns anos. Portanto, nossas empresas e nossos cidadãos estão constantemente sob essa ameaça.

Esses e-mails podem se passar por promoções imperdíveis em lojas conhecidas, bancos (informando operações realizadas, bloqueio de senha, etc), mensagens de sistemas, entre outros, sendo muitas vezes e-mails genéricos, que poderiam ter como alvo qualquer pessoa. São enviados para uma grande quantidade de usuários e, ao cair no phishing, a vítima acaba passando dados confidenciais, credenciais ou mesmo baixando artefatos maliciosos.

Mas nem sempre o phishing é genérico. Muitas vezes eles são direcionados para alvos específicos, utilizando informações verdadeiras sobre a vítima ou sobre o dia a dia dela.

Com essas informações precisas sobre a vítima, eles fazem a mensagem parecer mais real, tornando o phishing mais perigoso e mais eficiente.

Esse tipo de phishing é comumente direcionado à empresas, com o objetivo de comprometê-las.

Como identificar um phishing?

Sempre que receber uma mensagem, desconfie se:

- Você desconhece o remetente
- O contato estiver diferente do habitual
- Houver um tom muito impessoal
- Houver um tom de urgência, como “participe agora”, “preciso de ajuda urgente”, etc

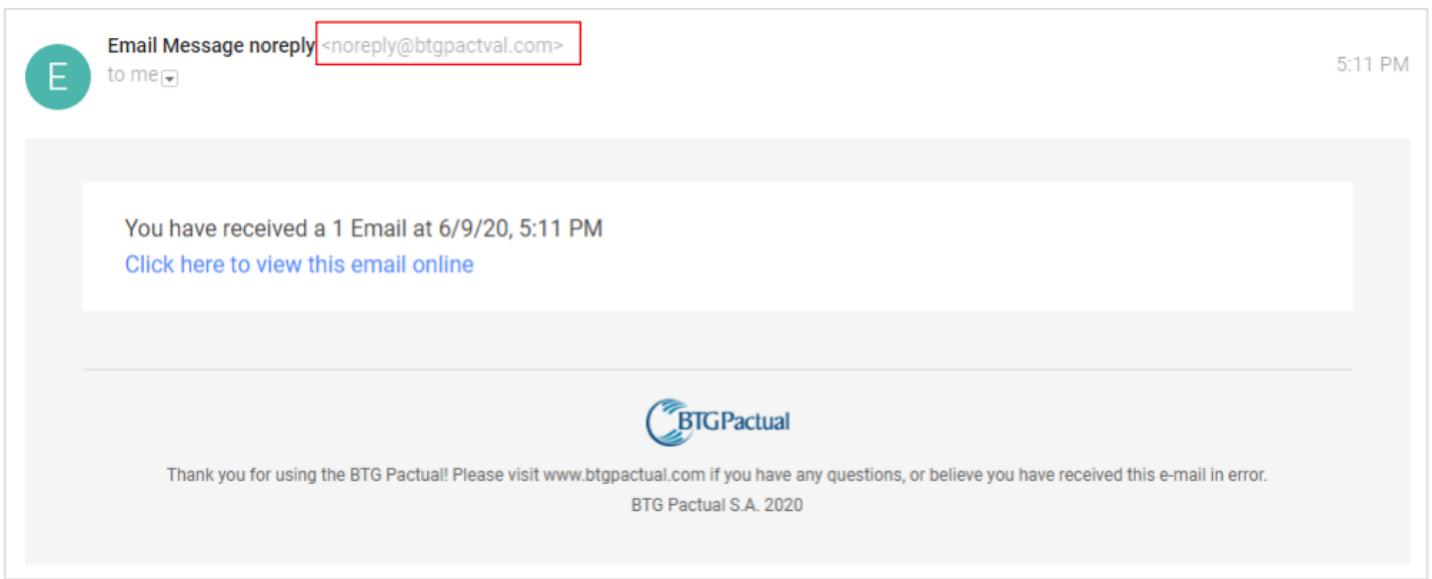
Fique atento!

- Criminosos podem criar e-mails muito parecidos com um e-mail legítimo, trocando ou omitindo algumas letras
- Se o assunto envolver pagamentos ou resgate valores, sempre se certifique através de outro canal que você realmente está falando com a pessoa certa
- Se receber uma mensagem suspeita de uma loja, prefira entrar no site pelo navegador (sem clicar em links da mensagem) e verificar se aquela promoção realmente existe ou se foi realmente feita alguma transação em sua conta

A seguir, veremos alguns exemplos de e-mails falsos e vamos aprender a identificá-los

Phishing

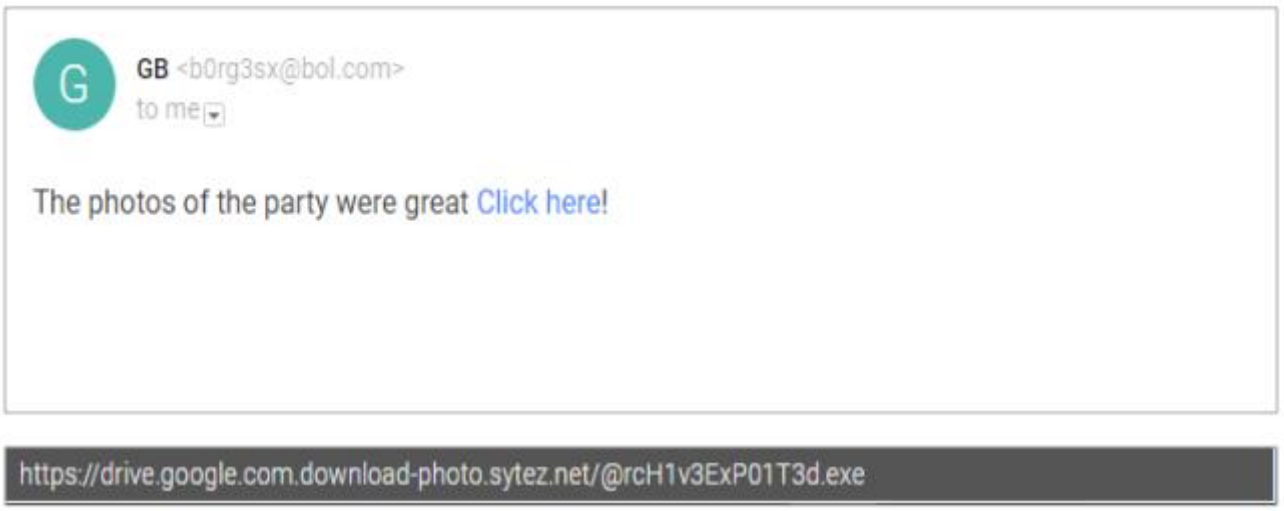
Observe a imagem abaixo:



Note que o domínio é muito parecido com o original, porém teve uma letra trocada. Portanto, essa mensagem se trata de um phishing.

Phishing

Observe a imagem abaixo:



Essa mensagem se trata de um phishing.

Note que o assunto tratado no e-mail é impessoal e provavelmente não esperado.

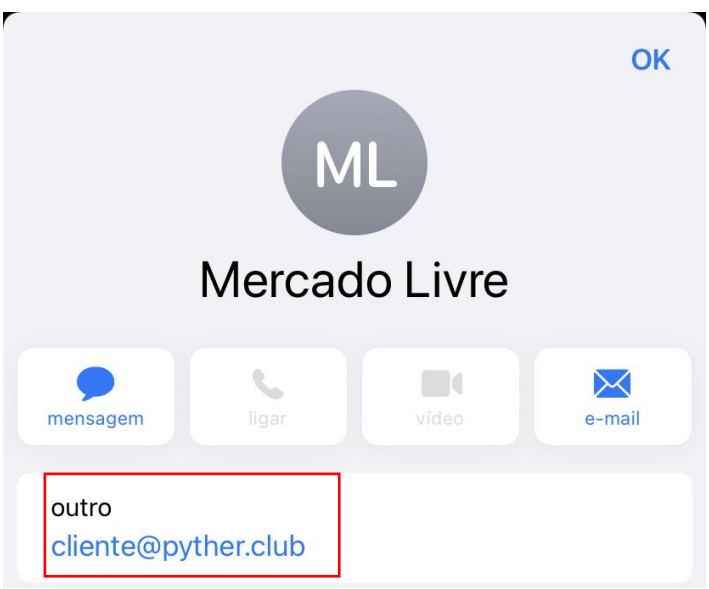
Ao passar o mouse sobre o link “click here” observamos que esse link direciona para uma URL onde será baixado um executável (observe o .exe no final do link na imagem cinza).

Esse phishing não direciona para um drive onde contém fotos e sim para um artefato malicioso.

Phishing

Essa é uma mensagem recebida em um e-mail, visto de um aparelho celular. Note que o a mensagem é muito bem feita, como se fosse real, e o display do e-mail aparece o nome correto da loja. Porém, isso se trata de um phishing.

Ao clicar no remetente, percebemos que o nome do e-mail nada tem a ver com a loja em questão. Isso pode ser um pouco mais difícil de conferir no celular, mas é importante sempre verificar.
Além disso, a não ser que você tenha anunciado um produto por esse valor, a mensagem não era esperada.



BEC

Uma modalidade de ataque que vem acontecendo e lesando milhares de empresas é o BEC (Business Compomise E-mail). Nesse caso, existe uma comunicação legítima entre duas partes: a empresa e um cliente ou até mesmo outra empresa. Uma das pontas dessa comunicação é comprometida e credenciais são capturadas (esse comprometimento pode ocorrer via phishing).

É mais fácil comprometer um cliente, uma vez que ele não possui filtros anti-phishing tão bons no seu e-mail e muitas vezes não sabe identificar mensagens falsas.

Agora, com acesso a todas as mensagens trocadas, o cibercriminoso aprende detalhes importantes sobre operações financeiras: valores aproximados de transações, por onde são feitos pagamentos ou transferências, dias e horários comuns de resgate de valores.

Dessa forma, ele cria um e-mail muito parecido com a conta comprometida e inicia uma comunicação, que vai se parecer muito com uma operação habitual. O criminoso pede resgate de valores para a conta dele, envia boletos para pagamento ou mesmo solicita informações, caracterizando roubo de dados.

Por isso, é importante estar sempre atento, mesmo que as mensagens recebidas sejam comuns à sua rotina e que o e-mail pareça um contato com quem você tem o costume de trocar mensagens.

Golpes do WhatsApp

Golpes no WhatsApp tem se tornado muito recorrentes. Existem alguns tipos de golpe:

- Uma pessoa com outro número de telefone se passa por você e entra em contato com seus amigos e parentes via mensagem no WhatsApp, usando a sua foto como foto de perfil. Os fraudadores geralmente inventam uma situação para fazer com que os contatos da vítima façam depósitos, pedindo dinheiro "emprestado" para os seus contatos. Eles, em geral, dizem "troquei de celular" ou "meu celular está no conserto" para justificar o fato de estar usando um número de telefone diferente do que você tem registrado. E usam desculpas como "atingi o limite de transações diárias", "preciso fazer um pagamento urgente e ainda não configurei o app do meu banco nesse celular", "estou em uma reunião e preciso fazer uma transferência urgente".

- Outra maneira, é o "sequestro" do WhatsApp, onde a sua conta é transferida para o aparelho do fraudador. Dessa maneira, ele consegue falar com pessoas através do seu número e você perde acesso ao app. Eles fazem essa transferência de aparelho através do SIM SWAP, uma fraude onde o seu número é ativado em outro chip, ou mesmo aplicando uma engenharia social na vítima fazendo ela passar códigos que chegam via SMS. Esses códigos na verdade são os criminosos solicitando a transferência da conta para outro aparelho.

- Fraudadores entram em contato via WhatsApp se passando por lojas ou órgãos do governo e solicitando dados pessoais, dados bancários, senhas, etc.

Como não ser vítima desse golpe?

Siga sempre essas dicas:

- Para evitar o sequestro da sua conta do Whatsapp, ative a autenticação em dois fatores em Configurações > Conta > Confirmação em duas etapas. Você escolherá um PIN e toda vez que você quiser trocar o Whatsapp de aparelho celular esse PIN será solicitado. Ele também é solicitado periodicamente durante o uso do app. Isso evitará que um fraudador consiga ativar a sua conta de Whatsapp em outro aparelho.
- Escolha uma foto para o Whatsapp diferente das suas outras redes sociais e configure para que a sua foto apareça apenas para os seus contatos. Para fazer isso acesse Configurações > Conta > Privacidade > Foto do Perfil e selecione a opção “Meus contatos”. Dessa maneira, os fraudadores terão mais dificuldade em copiar a sua foto e seus contatos irão perceber que as fotos estão diferentes.
- Desconfie de mensagens de órgãos oficiais do governo pedindo códigos ou qualquer informação via Whatsapp ou telefone. Esse tem sido um golpe recorrente, principalmente relacionado à vacinação contra o COVID-19.

Caso estejam se passando por você, envie uma mensagem para o suporte do Whatsapp (**support@whatsapp.com)** com o maior número de informações possível, solicitando ajuda

btg pactual

Outras dicas importantes

- Use senhas fortes, com caracteres maiúsculos, minúsculos, números e caracteres especiais sempre que puder
- Não compartilhe suas senhas com ninguém
- Não utilize informações pessoais nas suas senhas, como data de nascimento, por exemplo
- Habilite o duplo fator de autenticação sempre que puder, inclusive em e-mail e redes sociais
- Cuidado com as mensagens que recebe, seja via e-mail, whatsapp, etc; Se a conversa envolve valores, prefira conversar por telefone para garantir a identidade da pessoa com quem está falando
- Sempre faça as atualizações de segurança do seu celular, computador e outros aparelhos pessoais
- Mantenha um antivírus no seu computador


btg pactual