A QUANTINFOR APRESENTA...

Comece agora a travar o phishing!

Um guia para todos os colaboradores

Não caia no Isco

PHISHING É UM GRANDE NEGÓCIO

No último ano, ataques de phishing tiveram uma ascensão meteórica com os hackers a continuarem a refinar as suas táticas de ataque e partilhar diversos tipos de ataques bem sucedidos. Em particular, eles aproveitaram as ofertas de malware-as-a-service na "dark web" para aumentar a eficiência e o volume destes cibercrimes. Atualmente, 41% das organizações reportam ataques de phishing.

Como resolver este problema?

À MEDIDA QUE OS CIBERCRIMINOSOS CONTINUAM A ATACAR OS FUNCIONÁRIOS ATRAVÉS DA SUA TECNOLOGIA, ARGUMENTAMOS A FAVOR DA IMPORTÂNCIA DE UMA DEFESA POR CAMADAS: COMBINAÇÃO DE TECNOLOGIAS AVANÇADAS DE SEGURANÇA COM FUNCIONÁRIOS INSTRUÍDOS E CONSCIENTES.

LEMBRE-SE SEMPRE!

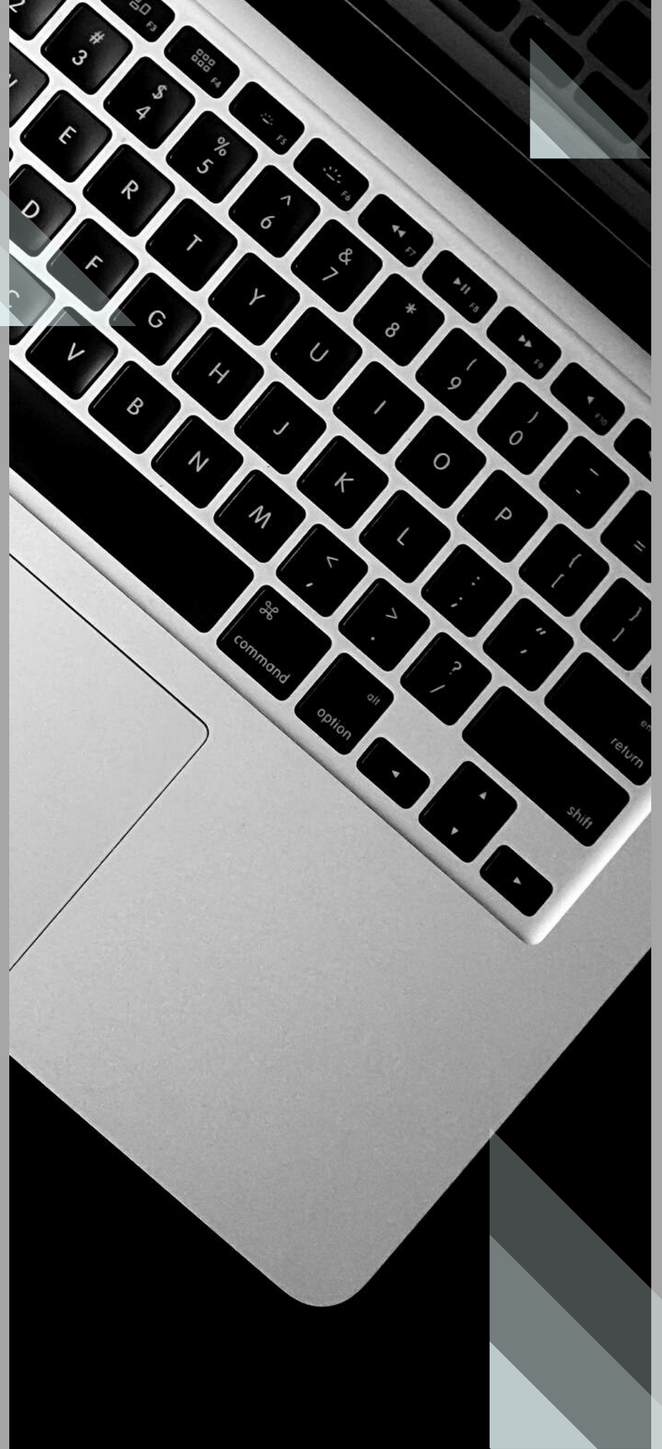
O PHISHING É UM GRANDE NEGÓCIO!

93% DAS VIOLAÇÕES DE DADOS INCLUEM PHISHING

Porque é que acontece?

A PRINCIPAL FORÇA POR DE TRÁS DE ATAQUES DE PHISHING É A RECOMPENSA FINANCEIRA

- 59% dos ataques são motivados por ganhos financeiros
- 41% dos ataques ambiciona obter dados de acesso não autorizados



Quem são os alvos destes ataques?

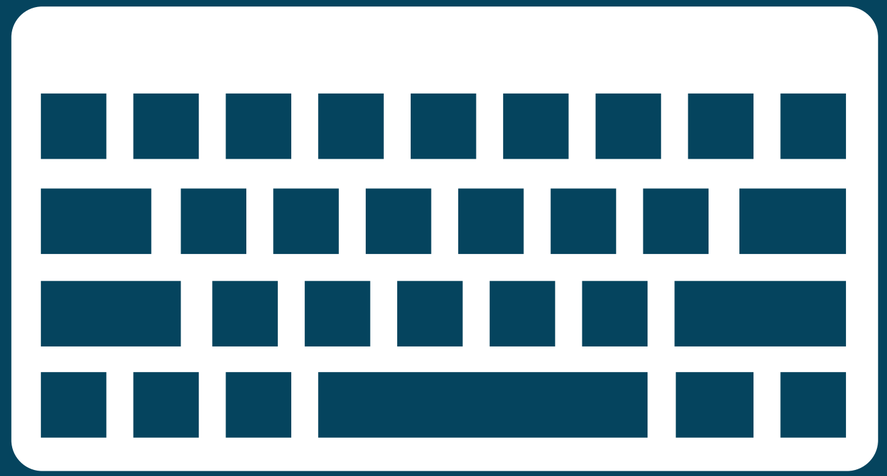
FUNCIONÁRIOS QUE TÊM ACESSO ÀS FINANÇAS DA EMPRESA, OU AQUELES QUE GEREM PROCESSOS DO NEGÓCIO

- 58% Departamento Contabilidade e Finanças
- 40% Departamento Administrativo e Gestão
- 23% Departamento de IT
- 22% Departamento de Vendas
- 18% Departamento de Recursos Humanos

89% dos ataques de phishing são elaborados por profissionais de crime organizado.

O QUE FAZ COM QUE A EFICÁCIA E PRODUTIVIDADE DOS MESMOS AUMENTEM

Estratégias de ataque evoluíram de tal forma que já há métodos de distribuição de ataques com kits de phishing.



Mas afinal como funciona o phishing?

O phishing abrange mais do que apenas falsos emails bancários e alertas de entregas de encomendas. Trata-se de convencer alguém a fornecer algo valioso aos atacantes. E o que começou como um simples “phishing” desenvolveu-se agora para 3 tipos de ataques: os clássicos, phishing em massa e spear phishing, e o business email compromise, subgrupo de spear phishing.

Tipos de Phishing

PHISHING EM MASSA

São em grande parte oportunistas, aproveitando o nome da marca para tentar atrair os clientes da empresa para sites falsos onde são levados a usar informações de cartão de crédito, credenciais de login, e outras informações pessoais que serão revendidas posteriormente para obter ganhos financeiros.

SPEAR PHISHING

Aqui são enviados emails personalizados fazendo-se passar por um determinado remetente ou de uma fonte confiável, são enviados para colaboradores específicos dentro das organizações para tentar fazer com que eles realizem determinadas ações, como enviar dinheiro para contas falsas.

BUSINESS EMAIL COMPROMISE

Os ataques de business email compromise são assim chamados porque estão associados a contas de email de funcionários que serão comprometidas em vez de o endereço do remetente ser falsificado. Isto torna os ataques muito mais difíceis de detetar pelos utilizadores finais.

3 Formas de lutar contra o Phishing:

VISIBILIDADE E EDUCAÇÃO

Através de simulações de phishing e formações.

ANTES DA ENTREGA DO EMAIL:

Secure Email Gateway

APÓS A ENTREGA DO EMAIL

Proteção de Endpoint

30% dos emails de phishing são abertos!

Visibilidade e Educação

Na luta contra o phishing, os utilizadores são o elo mais fraco. Na verdade, leva em média apenas 16 minutos para alguém clicar num email de phishing [Fonte: Verizon 2018 Data Breach Investigation Report]. Com os utilizadores na linha da frente dos ataques de phishing, é fundamental consciencializar e formar as pessoas de como identificar e evitar emails de phishing. Existem 3 etapas para uma simulação efetiva de phishing e um programa de formação:

- TESTAR: enviar simulações de phishing para testar a consciencialização do utilizador
- FORMAR: educar os utilizadores para parar com os ataques reais
- AVALIAR: acompanhar o progresso e melhoria de forma a orientar a formação

Antes da Entrega do Email

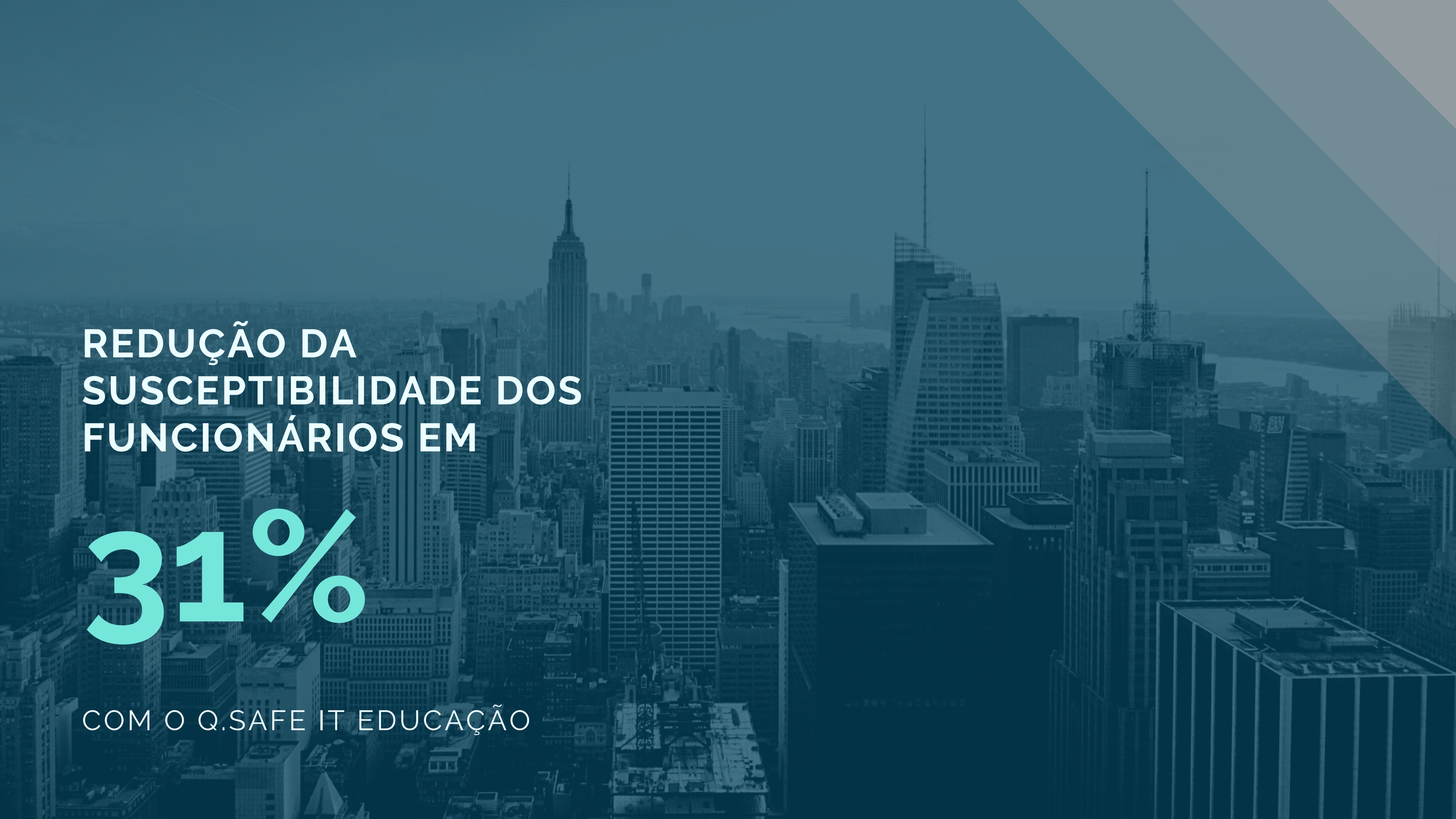
58% dos emails é spam e 77% de todos os spams contêm um ficheiro malicioso. Como resultado, um gateway de email seguro é um elemento essencial na luta contra o phishing. Ou seja, parar emails de phishing antes que eles entrem na sua caixa de entrada. As principais tecnologias utilizadas incluem:

- ANTI SPAM: Poderosas armadilhas de spam por todo o mundo, impedem que os emails cheguem aos utilizadores.
- REPUTAÇÃO DO REMETENTE: filtragem de reputação de IP para bloquear emails indesejados no gateway.
- AUTENTICAÇÃO DO REMETENTE: Deteta falsificação do remetente, anomalias no cabeçalho, e suspeitas do conteúdo do corpo do email.
- SANDBOXING: Deteta ficheiros suspeitos fora da rede
- BLOQUEIO DE URLS MALICIOSOS: Filtro de links maliciosos

Após a Entrega do Email

Uma proteção eficaz no endpoint é a linha final de defesa que protege a sua organização se um utilizador clicar num link malicioso ou abrir um anexo infetado. Procure uma solução de segurança de endpoint que ofereça técnicas fundamentais e modernas que incluem:

- DEEP LEARNING: Bloqueia ameaças desconhecidas de entrarem na organização
- ANTI-EXPLOIT: Impede que os atacantes explorem vulnerabilidades em softwares legítimos
- ANTI RANSOMWARE: Para encriptação não autorizada dos ficheiros da sua empresa



REDUÇÃO DA SUSCEPTIBILIDADE DOS FUNCIONÁRIOS EM

31%

COM O Q.SAFE IT EDUCAÇÃO

NÃO CAIA NO ISCO!
DE QUE FORMA?

PLANEIE AS SUAS SIMULAÇÕES DE PHISHING

FORME OS SEUS COLABORADORES

AVALIE OS SEUS PROGRESSOS E MELHORE A SEGURANÇA DA SUA EMPRESA

EM RESUMO:

Fique alerta aos 10 sinais que lhe apresentamos a seguir

SIMPLESMENTE NÃO PARECE CERTO

Há algo fora do comum com uma mensagem de email particular? Parece demasiado bom para ser verdade? Confie nos seus instintos.

SAUDAÇÕES GENÉRICAS

Em vez de se dirigir diretamente a si, os emails de phishing geralmente usam nomes genéricos como “Caro cliente.” Estas saudações impessoais poupam tempo aos cibercriminosos.

LINKS PARA SITES QUE PEDEM PARA INSERIR DADOS CONFIDENCIAIS

Estes sites falsos são muito convincentes, portanto fique atento a qualquer informação pessoal ou confidencial que lhe pedem para revelar.

EMAILS INESPERADOS QUE USAM INFORMAÇÃO ESPECÍFICA SOBRE SI

Informações como cargos, empregos anteriores, ou interesses pessoais podem ser obtidos em sites de redes sociais como é o cado do LinkedIn e são utilizados para tornar o email mais eficaz.

MÁ GRAMÁTICA OU ORTOGRAFIA

Sintaxe incorreta é sinal de que alguma coisa está errada. Significa, normalmente que é uma oferta falsa, que não tem qualquer efeito.

ENFRAQUECER PALAVRAS

Os hackers usam normalmente palavras enervantes, como por exemplo dizer que a sua conta foi violada, para o induzir a movimentar-se rapidamente sem pensar ao fazê-lo e revelar assim informações que normalmente não o faria.

SENSO DE URGÊNCIA

“Se não responder dentro de 48 horas, a sua conta será encerrada.” Ao criar um senso de urgência, os hackers esperam que cometa um erro.

"VERIFIQUE A SUA CONTA!"

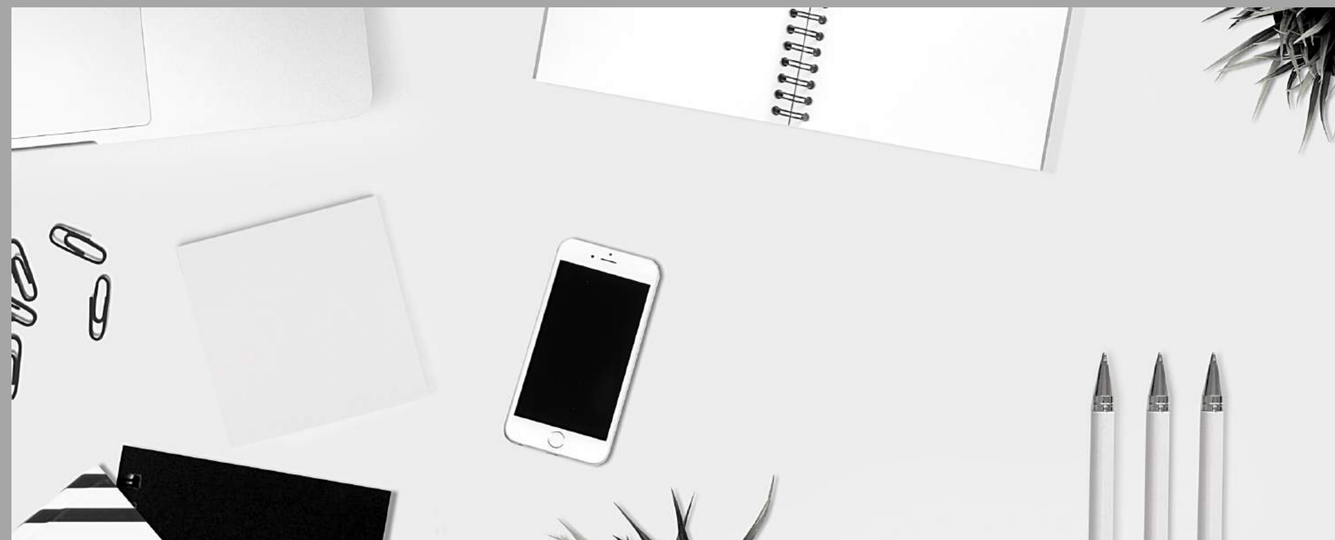
Estas mensagens falsificam emails reais e pedem que verifique a sua conta. Procure sempre sinais de phishing, e questione sempre porque é que essa verificação está a ser pedida, a probabilidade de ser fraude é elevada.

"GANHOU O GRANDE PRÉMIO!"

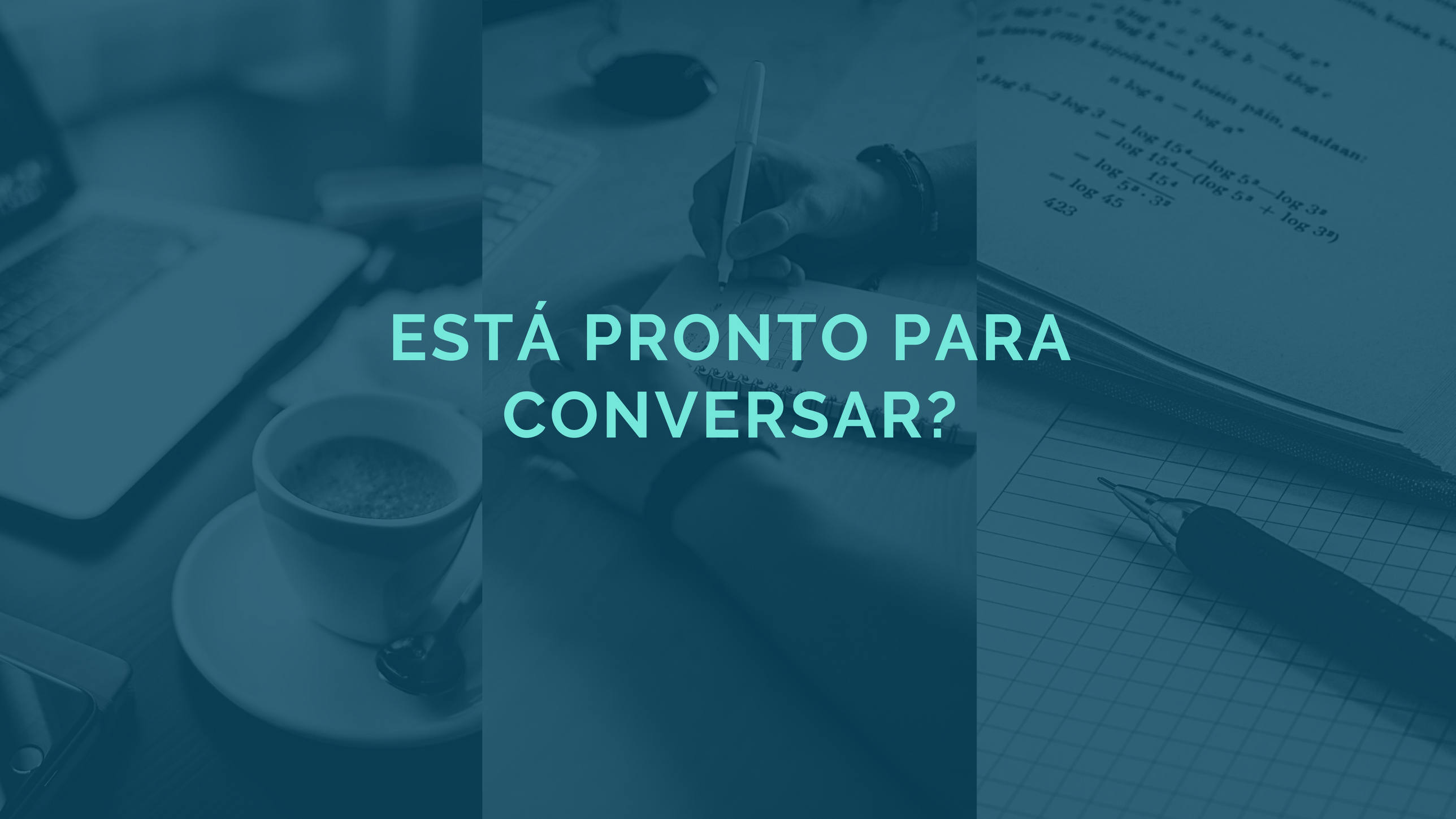
Estes emails de phishing são comuns, mas fáceis de detetar. Um dos exemplos é quando pede para que complete um questionário (dando assim as suas informações pessoais) em troca de um prémio.

CIBERSQUATTING

Muitas vezes, os cibercriminosos irão comprar domínios/nomes que são similares aos oficiais na esperança que os utilizadores acedam, como por exemplo:. www.google.com vs. www.g0ogle.com.
Avalie sempre o URL antes de inserir as suas informações pessoais.



Numa altura em que os casos de phishing relacionados com a pandemia de Covid-19 aumentam exponencialmente é essencial apostar na prevenção dos ataques às organizações dando os conhecimentos devidos aos seus colaboradores para evitar comportamentos de risco e por conseguinte evitar que os dados da sua empresa sejam comprometidos.



ESTÁ PRONTO PARA CONVERSAR?


COMECE AGORA!

Q.SAFE IT

www.qsafeit.com

CONTACTE-NOS E CONHEÇA A NOSSA MARCA Q.SAFE IT

Envie-nos um email para comercial@quantinfor.com e nós iremos ajudá-lo a lutar contra o phishing.

FONTE:

SOPHOS