Os mais procurados: os ciberataques que ameaçam o seu negócio

Os 10 ciberataques mais perigosos

Os ciberataques são um problema enorme. Custaram, a vítimas de todo o mundo, a dolorosa quantia de 9 bilhões de euros só em 2023. E podem passar por isso empresas de todos os tamanhos.

Neste guia inumeramos e analisamos as principais fraudes a que deve estar atento e explicaremos do que necessita para proteger a sua empresa e a sua equipa perante elas.

brother
at your side

A maioria dos ciberataques são cometidos contra pequenas e médias empresas.

60% das pequenas empresas vítimas de um ciberataque fechou num prazo de 6 meses*.
Uma estatística verdadeiramente impactante, não concorda?

E inclusivamente se a sua empresa sobreviver a um destes ataques, as implicações de o ter sofrido podem chegar muito longe, começando pelas perdas económicas e de credibilidade.

Com tantas repercusões importantes, fizemos uma lista das fraudes cibernéticas mais ameaçadoras e exploramos os fatores que melhor podem ajudar as empresas a fazer-lhes frente.

Segundo uma pesquisa recente realizada pela Brother, os responsáveis pelas decisões de TI não se sentem devidamente equipados para gerir alguma das ciberameaças mais comuns.
O *malware,* o *ransomware* e os ataques de *phishing* são as principais.

Manter a segurança nos sistemas de TI é outra dificuldade que costumam mencionar. De facto, 44% dos entrevistados considera que a gestão destes sistemas é o seu maior desafio.

Por isso a Brother está ‘At your side’ para ajudar.

Encontrar a informação prática que necessita, quais são os riscos, como identificá-los e como permanecer seguro não é fácil.

Neste documento revelamos algumas das fraudes cibernéticas mais invulgares e impactantes que deve conhecer, e compilamos a informação e as ferramentas que pode utilizar para se manter seguro sem que interfiram no seu dia-a-dia.

Dê uma vista de olhos à nossa lista dos 10 "Mais Perigosos" ciberataques e adiante-se aos riscos mais ameaçadores que se escondem na internet.

*TechRound, março 2023

Sabia que…?

A marca mais suplantada é a Microsoft (29%), seguida pela Google (13%) e Amazon (13%).

A fraude

Um colaborador recebe uma mensagem, por norma um email, embora possa ser também uma mensagem no Microsoft Teams, de uma marca aparentemente fiável como Apple ou Google.

Como muitas destas fraudes, a mensagem dirá que é necessária uma ação URGENTE, como introduzir ou enviar informação da sua conta, um pagamento ou as suas palavras-passe.

Infelizmente, a maior parte destas ameaças que utilizam o *phishing* como meio, normalmente baseiam-se em fazer-se passar por marcas bem conhecidas como Microsoft, Amazon, DocuSign ou Google para enganar os utilizadores. De facto, só em 2022 foram detetadas mais de 30 milhões de mensagens utilizando a marca Microsoft ou mencionando produtos Microsoft em ataques de *phishing*.*

Possíveis consequências para o negócio

Mesmo com pequenas informações os hackers podem conseguir os dados que necessitam para aceder às contas dos seus clientes, roubar palavras-passe e, no fim de contas, roubar dinheiro.

Ofereça a toda a equipa formação regular em cibersegurança, dando especial atenção a como identificar links suspeitos. Basta um clique para desencadear a catástrofe.

Porque caímos

Este tipo de ameaça baseia-se na familiaridade e confiança que temos nas marcas com as quais trabalhamos diariamente. Isso, juntamente com a aparente urgência requerida, é a razão que atrai os colaboradores.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos
- Confirme o endereço de email (tem o formato correto da organização à qual diz pertencer?)
- Parece um email genuíno da marca?
- Vigie as mensagens do Microsoft Teams que pareçam suspeitas
- Verifique se há erros gramaticais evidentes
- Duvide da urgência, esse é sempre um alerta vermelho

*Forbes, março 2023

O facto de o LinkedIn ser uma rede social profissional não o torna mais seguro.

A fraude

O LinkedIn é o principal alvo das fraudes através de *phishing*. Os impostores utilizam táticas como ofertas de trabalho falsas, conversas falsas sobre conexões pessoais e inclusivamente potenciais relações românticas. Estas burlas, desenhadas para enganar os utilizadores para que revelem informação sensível, são cada vez mais comuns. E assim que o impostor conseguir ganhar a confiança de alguém, será muito mais fácil extrair-lhe informação valiosa.

Possíveis consequências para o negócio

Os impostores pedirão dados pessoais ou enviarão *malware* disfarçado de documentos supostamente importantes, o que lhes permitirá ter acesso a mais dados, arquivos valiosos ou inclusivamente às contas bancárias da empresa.

Porque caímos

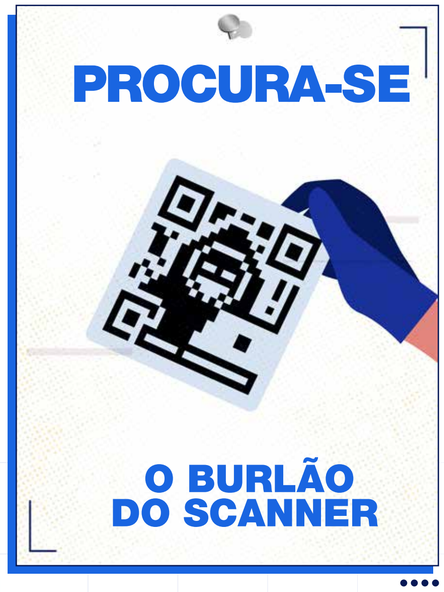
Este tipo de fraude baseia-se na confiança que temos numa plataforma profissional como o LinkedIn. Os burlões podem, por exemplo, fazer-se passar por recrutadores, prometendo grandes benefícios e aproveitando-se do interesse das pessoas por trabalhar a partir de casa.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos e assegure-se de que estão alerta inclusivamente quando são contactados nas redes sociais.
- Duvide de mensagens não solicitadas.
- Verifique qualquer ficheiro que lhe tenham pedido para descarregar.

Um estudo recente de Check Point Research* revela que o LinkedIn é a marca com mais impostores a utilizar ataques de *phishing*.

*Infosecurity Magazine, abril 2022



Peça à sua equipa que desconfie de códigos QR que cheguem em emails para que efetuem uma autentificação multifator.

A fraude

Os códigos QR estão em todo o lado. Por isso, se um colaborador recebe um email pedindo-lhe que digitalze um, poderia não pensar duas vezes. Mas nem todos os códigos QR são seguros.

Pode haver códigos falsos em qualquer parte, mas alguns dos lugares mais comuns para isso podem ser emails (falsos) de autenticação multifator ou de recuperação de documentos ou, inclusivamente, em público.

Há pouco tempo uma mulher perdeu 15.000€ por uma fraude deste tipo ao usar um código QR falso para pagar um parque de estacionamento. Esse código levou a vítima, de 71 anos, a uma página web falsa onde preencheu os detalhes de pagamento e isto permitiu aos malfeitores roubar os seus dados pessoais e a informação do cartão*.

Possíveis consequências para o negócio

Os códigos QR não seguros podem dirigir os colaboradores a páginas web corporativas falsas, sites de pagamento não legítimos e redes maliciosas. Também podem introduzir um código malicioso nos seus dispositivos de maneira inadvertida para conseguir roubar dinheiro e dados sensíveis da empresa.

*Independent, novembro 2023

Porque caímos

As empresas utilizam sistemas de autentificação multifator todos os dias, especialmente quando usam sistemas como Microsoft. As pessoas estão habituadas a introduzir os seus dados, pelo que muitas vezes não pensam duas vezes quando recebem um email que lhes pede para fazê-lo.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre dos perigos.
- Pense antes de o digitalizar. Não atue de forma impulsiva
- Pré-visualize o link do código QR.
- Não leia códigos QR que recebe de forma inesperada ou que provenham de pessoas ou empresas estranhas.
- Perante a dúvida, contacte a empresa que supostamente está a enviar esse código.

Dar acesso a toda a equipa à conta bancária corporativa é cómodo, mas tem os seus riscos. Este tipo de fraude custou milhões a muitas empresas nos últimos anos.

A fraude

Neste tipo de fraude os criminosos fingem ser o banco no qual tem a sua conta e tratam de lhe roubar dinheiro. E este é um problema comum tanto a particulares como a empresas: estima-se que metade dos adultos recebe mensalmente pelo menos uma mensagem de *phishing* deste tipo.

Os malfeitores contactarão a sua empresa por telefone, mensagem de texto ou email, muitas vezes alegando que há uma transação suspeita que necessita ser verificada. Pedirão que clique num link que abre uma página de acesso falsa e a partir daí roubarão as suas palavras-passe para aceder à sua conta verdadeira. Alguns inclusivé chegam a utilizar falsas aplicações bancárias.

A marca de cabeleireiros Kent Brushes sabe disso muito bem, já que perdeu 1,8 milhões de euros em 20 minutos. Os ladrões enganaram um dos seus colaboradores para que lhes desse acesso à conta da empresa e o resto, como se costuma dizer, é história*.

Possíveis consequências para o negócio

Uma vez que o cibercriminoso tem acesso a uma conta, pode hackear muito mais, incluindo emails ou contas bancárias.

*BBC.co.uk, outubro 2023

Porque caímos

As empresas, tal como as pessoas, confiam no seu banco. Também têm medo de ser vítimas de uma fraude, pelo que podem acreditar na história de uma ‘transação suspeita’.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Lembre-se: o seu banco nunca pedirá palavras-passe ou que efetue transferências de dinheiro para outras contas.
- Nunca envie dados bancários por mensagem de texto.
- Não clique em links que lhe cheguem de forma inesperada ou que pareçam suspeitos.
- Procure erros gramaticais nas páginas de acesso ao banco.

Ninguém está a salvo de ser enganado por um vigarista. Inclusivamente poderiam dirigir-se ao seu CEO, porque quanto mais ocupada está a pessoa, mais provável será que caia no esquema.

A fraude

Se calhar já ouviu falar de uma fraude chamada *'pretexting'*. É quando um cibercriminoso se faz passar por uma pessoa real (normalmente um membro sénior da empresa) e utiliza um discurso credível para enganar um colaborador.
Alguns chegam inclusivamente a utilizar clips de audio.

Pedirão ao colaborador que lhes dê informação sensível ou inclusivamente dinheiro, muitas vezes ameaçando-os que o seu trabalho depende disso.

Possíveis consequências para o negócio

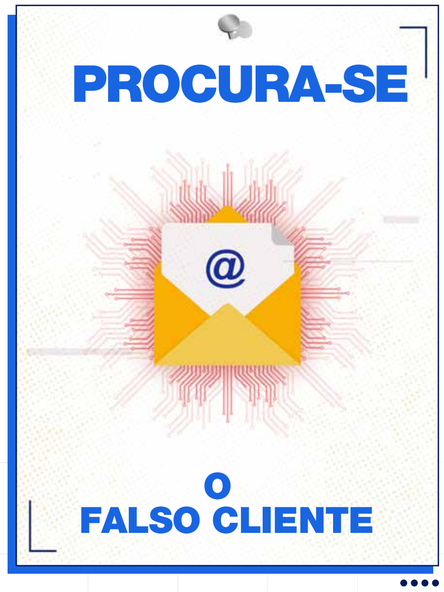
Estes criminosos fazem as suas investigações e utilizam informação precisa e verdadeira que encontraram online ou em qualquer outro sitio. Podem reforçar o seu engano usando números de telefone e endereços de email falsos. E isto pode custar à empresa muito dinheiro.

Porque caímos

Este tipo de fraude baseia-se no nosso medo da autoridade e de perder o trabalho. Além de parecer verídico porque utilizam informação real e uma narrativa plausível.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Pare e pense sempre antes de atuar.
- Nunca envie detalhes bancários através de uma mensagem de texto.
- Pense se a história faz sentido.
- Contacte a pessoa real mediante outro meio de comunicação para verificar os conteúdos do potencial vigarista.



Qualquer colaborador que lide com dinheiro da empresa de forma regular (inclusivé para pequenos gastos do escritório como papelaria) pode beneficiar de uma formação sobre como identificar emails ou outras mensagens falsas.

A fraude

Conhecido formalmente como *Business Email Compromise* (BEC) neste tipo de fraude um criminoso faz-se passar por um possível cliente enviando emails bastante realistas a colaboradores específicos. Podem conter pagamentos invulgares, conter links para websites falsos ou simplesmente pedir informações sobre algum produto, que depois será comprado utilizando cartões de crédito roubados.

Ao contrário dos emails de *phishing* mais comuns, que são enviados massivamente a milhões de pessoas, os ataques BEC estão desenhados para enganar indivíduos concretos, o que os torna mais difíceis de detetar.

Possíveis consequências para o negócio

Todas as empresas, grandes e pequenas, estão em risco. 29% das empresas afirma ter perdido clientes devido a um ataque BEC*.

MGM Resorts foi vítima de uma fraude BEC que lhes levou a ter que suspender todo o seu sistema informático, o que implicou um custo de 100 milhões de euros**.

Utilizando informação encontrada num post do LinkedIn, um cibercriminoso fez-se passar por um colaborador da MGM e telefonou ao departamento de TI pedindo-lhes para efetuarem um reset à sua palavra-passe. Para o fazerem, estavam a dar aos atacantes acesso a essa conta de colaborador e, a partir daí, aceder a todo o sistema da empresa.

Tudo, desde as chaves digitais do hotel até às máquinas de jogo, deixou de funcionar e a internet de muitos dos seus estabelecimentos caiu. Os hóspedes tiveram que esperar em longas filas para fazer o *check-in,* utilizar chaves físicas para os quartos ou manusear recibos manuais dos seus ganhos nos casinos, já que a empresa passou para o modo manual para continuar a ser o mais operacional possível enquanto se resolvia o problema.

Porque caímos

Os malfeitores atraem as pessoas da empresa susceptíveis de lidar com dinheiro. Aproveitarão a preocupação com os custos, explorarão qualquer incerteza em termos de rentabilidade e dirigir-se-ão a empresas muito orientadas para as vendas e pagamentos.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Cumpra os seus processos oficiais relativos às transacções financeiras.
- Suspeite de emails de organizações com as quais não tem relação.
- Não perca de vista a informação que está disponível publicamente.
- Verifique que as pessoas são quem dizem ser.
- Utilize diferentes palavras-passe para as suas contas.
- Duvide de qualquer urgência.

*Security Infowatch, março 2022 **Reuters.com, outubro 2023

Todas as impressoras da Brother são seguras de série, já que oferecem uma segurança a três níveis: rede, dispositivo e documento.

A fraude

Mais de um em cada dez incidentes que afetam uma empresa estão relacionados com uma impressora*. Podia ser um filme de terror, mas quando os hackers atacam um hardware de impressão vulnerável é, pelo menos, caso para se assustar. Tomam o controlo dos equipamento de impressão e começam por imprimir mensagens como 'foi hackeado' para provar que se podem infiltar na sua rede. Depois, ameaçam em levar a situação mais além.

Possíveis consequências para o negócio

Para além de mostrarem as suas habilidades, esta é uma forma em que os criminosos podem tomar o controlo da sua rede e, portanto, lançar a partir daí ataques mais sofisticados. As impressoras podem ser um caminho para outros recursos mais importantes, como servidores de arquivos ou de email.

Porque caímos

As empresas vêem as impressoras como um dispositivo de baixo risco, mas isso está longe da realidade. Por elas passa informação sensível e os hackers podem vê-las como uma porta traseira sem vigilância para entrar numa organização.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Mantenha as suas impressoras fora do alcance de utilizadores não autorizados.
- Peça identificação nos interfaces de impressão.
- Utilize palavras-passe seguras.
- Solicite encriptação de ponta a ponta para que os dados enviados para as impressoras não sejam intercetados ou manipulados.
- Mantenha o firmware atualizado.

Com uma configuração de impressão segura, ninguém deveria ser capaz de obter acesso aos seus dispositivos. Assegure-se de que o firmware está atualizado e que todas as suas impressoras são seguras.

*Quocirca, outubro 2023

Desde instalar um software antivírus até garantir que o WiFi da empresa é seguro, manter os dados seguros é realmente importante.

A fraude

Este é provavelmente o golpe de perfil de maior visibilidade na lista dos 'Mais Perigosos'. Os criminosos dirigem-se a grandes empresas, frequentemente nos setores da saúde, financeiro e energia, e roubam grandes quantidades de dados pessoais sensíveis pelos quais 'pedem resgate'.

Utilizam emails de *phishing,* identidades roubadas e debilidades de segurança do sistema para encontrar a forma de entrar.

A Royal Mail teve um ataque de *ransomware* por parte de um grupo criminoso que ameaçou publicar a informação roubada online e deixou a empresa incapaz de enviar encomendas ou cartas para o estrangeiro*.

Possíveis consequências para o negócio

Na maioria dos países, as organizações estão legalmente obrigadas a proteger qualquer dado pessoal que tenham. As fugas de dados podem incorrer em importantes multas que podem sair muito caras para os negócios. Atualmente, o custo médio de uma falha de dados é de uns 5,1 milhões de euros **.

Uma das violações de dados mais sérias dos últimos tempos teve lugar no Reino Unido, quando os criminosos atacaram a Comissão Eleitoral e conseguiram aceder a informação pessoal de 40 milhões de pessoas. Não há evidência de que esses dados tenham sido explorados ou utilizados, mas o facto de que acederam a eles é prova suficiente de que a segurança da Comissão não era suficientemente forte ***.

Porque caímos

Os criminosos aproveitam-se de debilidades empresariais. Emails comprometidos, uma má configuração da nuvem, vulnerabilidades não corrigidas e a falta de formação são sempre formas de entrar.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Incorpore segurança em cada etapa do desenvolvimento e instalação do software e teste-a regularmente.
- Utilize tecnologias de segurança de dados e cumprimento de normas e standards que protejam o fluxo de informação entre bases de dados, aplicações e serviços.
- Tenha uma equipa profissional preparada e pronta para responder perante qualquer incidente e reduzir o impacto.
- Implemente formação e boas práticas de segurança de dados.

Ninguém está imune. Todos os dias conhecem-se novos relatórios sobre fugas de dados em algumas das maiores empresas do mundo. E muitas vezes levam também a elevadas multas ou inclusivamente a acusações legais.

*The Guardian, janeiro 2023 **IBM, janeiro 2023 ***bbc.co.uk, agosto 2023

Pode ser tentador vasculhar em documentos digitalizados de outras pessoas, mas não se deixe levar por isso (ocupe-se dos seus assuntos!)

A fraude

Um email aleatório, supostamente enviado desde uma impressora do escritório, diz que um colega recebeu um novo documento digitalizado. E todos os detalhes parecem genuinos. Pode inclusivamente ter uma mensagem a dizer que o documento foi digitalizado de forma segura e um sinal de copyright. Dois links dão-nos a opção de visualizar ou descarregar o documento. E isto é, na realidade, um email de *phishing.*

Possíveis consequências para o negócio

Os links, claro, vão levá-lo a uma página web falsa onde os malfeitores tratarão de extrair as palavras-passe do email, permitindo-lhes assim enviar spam, distribuir malware e inclusivamente aceder a informação financeira através delas.

Porque caímos

Esta fraude é perigosa porque provém de um equipamento do escritório que consideramos fiável. É também estranho que lhe envie um email e essa sensação de surpresa pode levar à partilha da informação.

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Duvide de anexos e links em emails inesperados.
- Apenas descarregue ficheiros de fontes fiáveis.
- Duvide de qualquer urgência.

As ferramentas de IA como ChatGPT estão a fazer com que os emails de *phishing* sejam mais difíceis de identificar e isto está a aumentar o risco para as empresas.

A fraude

Todos já sabemos como identificar um email de phishing: estão cheios de erros de ortografia e de gramática, certo? Pois, já não é bem assim. Os criminosos agora utilizam IA, ChatGPT e chatbots para compôr os seus emails de phishing com uma redação perfeita.

Possíveis consequências para o negócio

Como resultado da utilização da IA, as comunicações fraudulentas parecem mais autênticas, mais autoritárias e mais fiáveis. E uma vez que os criminosos ganhem confiança, conseguirão outros dados pessoais para se fazerem passar por indivíduos conhecidos ou aceder às suas contas. Já se registou um aumento de 1265% no número de emails de *phishing e* a IA tem muito a ver com isso*.

Porque caímos

Estes emails de *phishing* mais credíveis fazem com que as vítimas confiem e partilhem dados pessoais ou das suas contas.

*CNBC, novembro 2023

Como manter a empresa e a equipa seguras

- Mantenha toda a equipa informada e atualizada sobre os perigos.
- Tenha cuidado com a informação que os colaboradores partilham.
- Não difunda detalhes de registo nem palavras-passe.
- Tenha cuidado com os dados que estão publicamente disponíveis. Os atacantes podem usá-los contra si.
- Verifique que as pessoas são quem dizem ser.

Mantenha o seu negócio protegido contra os 10 ciberataques mais perigosos.

Agora que leu este guia, já sabe como identificar o comportamento, táticas e truques dos cibercriminosos.

Mas, tendo em conta que 60% dos pequenos negócios fecha, em média, seis meses depois de um ciberataque, é fundamental que continue a consultar este guia.

Tenha-o sempre à mão e partilhe-o com os seus colegas.

Com a Brother ‘At your side’ pode ir um passo mais à frente dos cibercriminosos e caminhar rumo a um futuro mais seguro para o seu negócio.

brother
at your side