

CIBERSEGURANÇA



#01 - O que é o Phishing

CIBERSEGURANÇA

Em parceria com a highdome,
especialista em segurança cibernética
para pequenas e médias empresas,
vamos disponibilizar-lhe todos os meses
conteúdos exclusivos para o sensibilizar,
a si e aos seus colaboradores,
a adotarem uma postura de prevenção
constante que permita fortalecer a
resiliência cibernética na sua empresa.

highdome
closing the cyber gap



AHRESP®

ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL

Instituição de Utilidade Pública

#01

O que é o Phishing

Phishing é um **crime cibernético** no qual um **alvo é contactado por e-mail**, por alguém que se faz passar por uma instituição legítima para induzir indivíduos a **fornecerem dados confidenciais**, como informações pessoais, detalhes bancários, de cartão de crédito, passwords e muito mais.

As informações são usadas para aceder a todo o tipo de contas, e podem resultar em roubo de identidade e perdas financeiras, para si e para a sua empresa.



#01 O que é o Phishing

Principais tipos de e-mails que caracterizam o Phishing

Bom demais para ser verdade:

ofertas lucrativas e declarações atraentes ou que chamam a atenção da vítima imediatamente.

Sentido de Urgência:

uma tática favorita entre os cibercriminosos é pedir que responda rapidamente às supostas super ofertas que geralmente são por tempo limitado.

Hiperlinks:

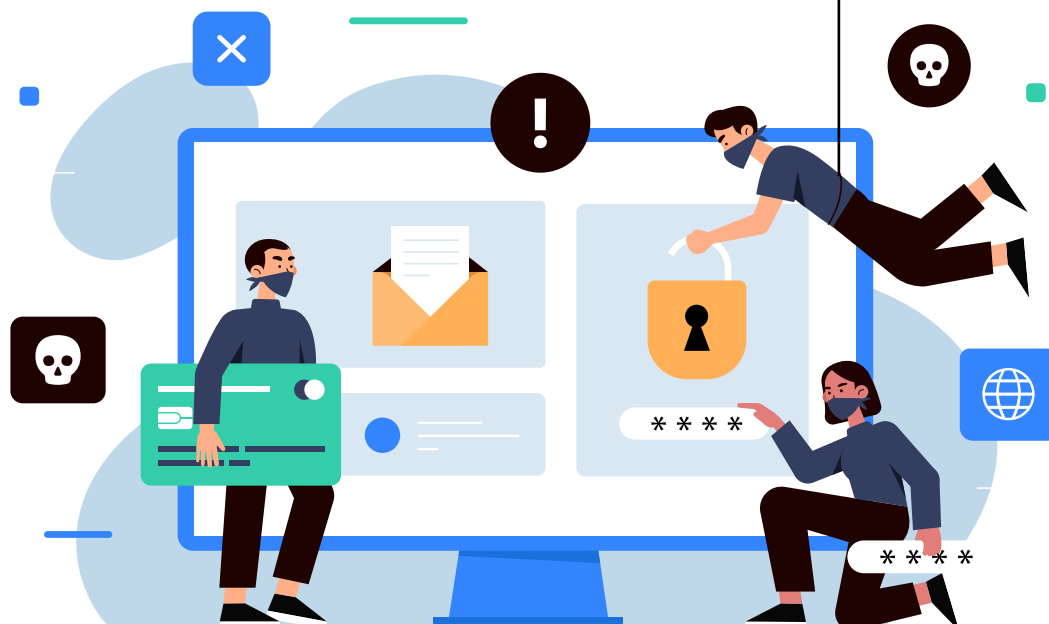
um link pode não ser tudo o que parece ser. Passar o rato sobre o link para ver o endereço real para onde será direcionado é uma boa prática antes de clicar.

Arquivos anexos:

se receber um anexo num e-mail que não esperava ou que não faz sentido, não abra!

Remetente desconhecido ou incomum:

esta é uma característica que requer muita atenção; se algo lhe parecer fora do comum, não clique!



#01 O que é o Phishing

Sempre que receber um e-mail preste muita atenção a estas informações.

1 FROM

- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

2 TO

- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

3 HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "y" and "n."

4 DATE

- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

5 SUBJECT

- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

6 ATTACHMENTS

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

7 CONTENT

- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

- 1 From - Quem envia** - É importante verificar se conhece o remetente do email; se é de fora da sua empresa e se conhece a empresa de onde veio; se nunca recebeu email destas entidades; e se tem hiperlinks ou anexos; e caso existam dúvidas não clicar em nada.
- 2 To - Quem recebe** - Verificar se está em CC e o email foi enviado para um conjunto de pessoas que não conhece e com um assunto que não é familiar.
- 3 Hiperlinks** - Analisar se o mesmo é válido, passando com o rato por cima do link e lendo o endereço; se o email que recebeu tem apenas um link longo e nada mais escrito no email, seguramente esse mail é não é normal; verificar se o link tem erros ortográficos, geralmente as instituições não cometem esses erros.
- 4 Data** - Verificar se o email recebido chega a uma hora anormal, como por exemplo às 03:00 da manhã; será normal receber o email deste remetente a esta hora?
- 5 Assunto** - Verificar se o assunto faz sentido com o email e se o reconhece; se é uma resposta a algo que nunca enviou.
- 6 Anexos** - Verificar se faz sentido o remetente enviar um anexo e se esperamos que ele o faça; verificar que tipo de anexo é, apenas os .TXT são seguros, os perigosos são: .EXE, .CDM, .BAT, .SCR, .VBS ...
- 7 Conteúdo** - Verificar a gramática, se tem erros; se tem sentido de urgência; se diz que fomos apanhados em algo ilegal ou embaraçoso; todos estes pormenores podem indicar um email de Phishing.

Partilhe sempre estas boas práticas com os colaboradores da sua empresa e até mesmo com familiares e amigos, de modo a evitar que possam ser alvo de um ataque cibernético.

#01 O que é o Phishing

Geralmente, os e-mails enviados por cibercriminosos são mascarados para que pareçam ter sido enviados por uma empresa cujos serviços são usados pelo destinatário.



Um banco não solicita informações pessoais por e-mail nem suspende a sua conta se não atualizar seus dados pessoais num determinado período de tempo.

A maioria dos bancos e instituições financeiras também costuma fornecer um número de conta ou outros dados pessoais no e-mail, o que garante que ele vem de uma fonte confiável.

Divulgue estes conselhos e partilhe-os na sua rede de contactos!

Caso queira aprofundar os seus conhecimentos e dos seus colaboradores consulte as informações sobre o Programa de Prevenção Cibernética da Highdome:

learn.highdome.io/prevencaocibernetica



CIBERSEGURANÇA



AHRESP[®]

ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL

Instituição de Utilidade Pública

highdome
closing the cyber gap