CIBERSEGURANÇA

#01 - O que é o Phishing

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

highdome
closing the cyber gap

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.

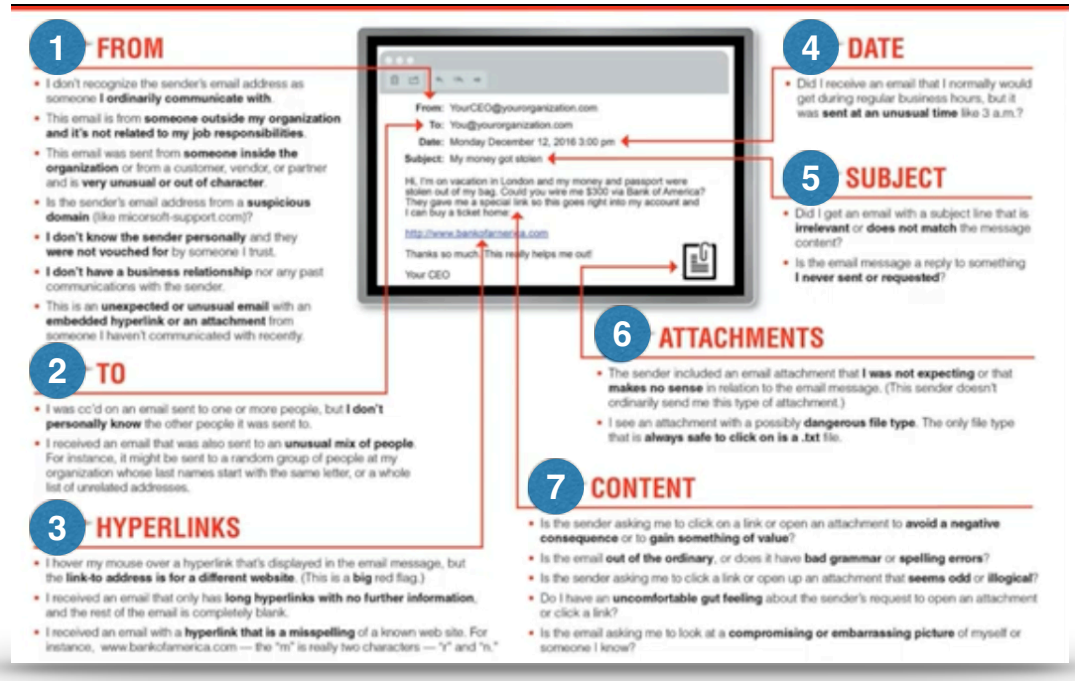
Hiperlinks:
um link pode não ser tudo o que parece ser. Passar o rato sobre o link para ver o endereço real para onde será direcionado é uma boa prática antes de clicar.

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 - 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 ás 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 este pormenores podem indicar um email de Phishing.

Partilhe sempre estas boas práticas com os colaboradoresda 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

AHRESP
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

highdome
closing the cyber gap

CYBERSEGURANÇA

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

highdome
closing the cyber gap