

# Phishing

JOÃO VITOR, JÚLIO BOTACCIO  
E KEREN STEVAUX



# topicos

O'QUE É PHISHING

TIPOS DE PHISHING

COMO FUNCIONA OS ATAQUES DO PHISHING

TÉCNICAS PARA PREVENIR ATAQUES DE  
PHISHING

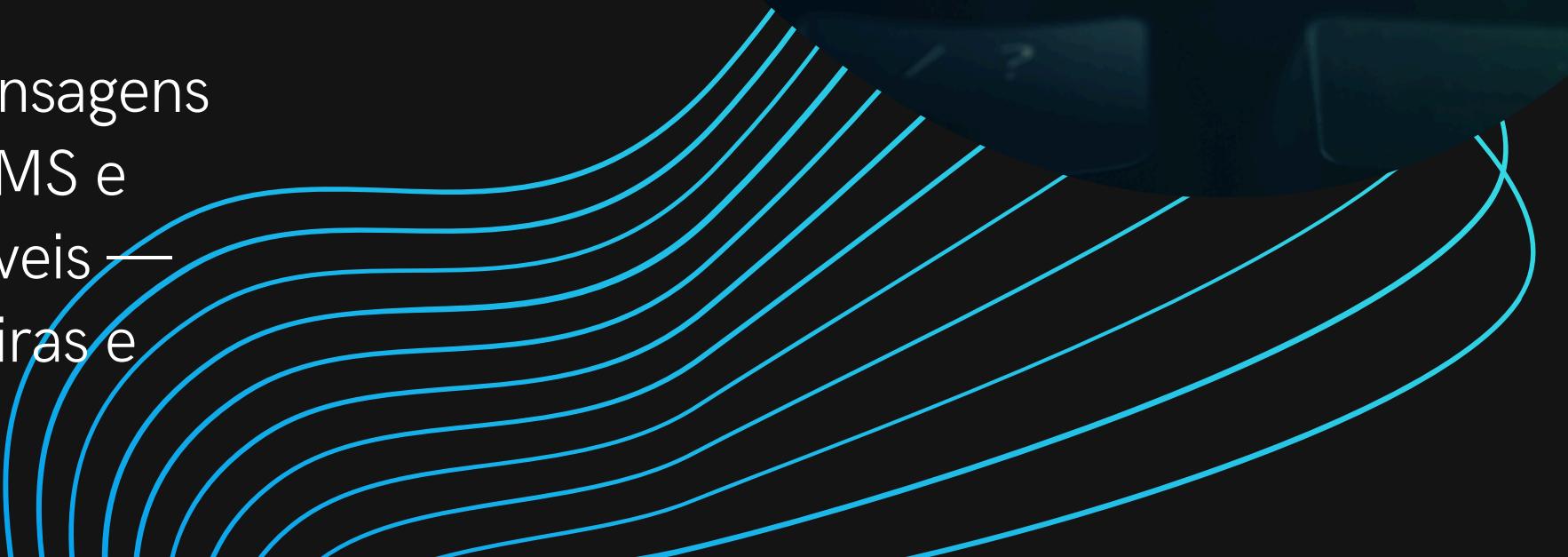
EXPERIÊNCIA DE TRABALHO 5

# O'que é Phishing

Phishing é o crime que enganar as pessoas, por meio de comunicações falsas, para que compartilhem qual quer dado dela, como senhas bancárias, número do cartão de crédito ou informações de login etc.

O nome se origina de um termo em inglês que é “fishing”, que significa “pescar”, fazendo alusão ao objetivo de obter uma forma ilegal de uma maneira manipuladora psicologicamente o usuário para a obtenção informações.

Na prática, os cibercriminosos enviam mensagens falsas, por meio de canais como e-mail, SMS e WhatsApp, se passando por fontes confiáveis — empresas renomadas, instituições financeiras e órgãos governamentais, entre outros.



# Tipos de Phishing



Scam:

- Objetivo: roubar dados pessoais de um grande número de usuários de forma indiscriminada.
- Método: comunicações genéricas enviadas para bases de contatos volumosas por e-mail, telefone, SMS e redes sociais.
- Estratégia: mensagens que ativam as emoções do usuário, usando ameaças, avisos urgentes e promessas de ofertas imperdíveis, com elementos textuais e visuais para parecerem legítimas.

Spear phishing:

- Objetivo: atacar grupos específicos, como funcionários de empresas ou órgãos governamentais.
- Método: comunicações personalizadas com detalhes específicos sobre as vítimas, como nomes, cargos e endereços de e-mail, para parecerem confiáveis.

# Tipos de Phishing



## Clone phishing:

- Objetivo: replicar e-mails legítimos trocando apenas o link ou anexo da comunicação.
- Método: a vítima recebe um e-mail clonado, sendo direcionada para baixar um arquivo malicioso ou acessar um site falso, comprometendo suas informações pessoais.

## Whaling:

- Objetivo: atacar executivos de alto nível, como CEO ou CFO de empresas.
- Método: comunicações referentes a notificações judiciais, queixas de clientes ou comunicados internos da empresa.

## Vishing:

- Objetivo: solicitar dados pessoais por meio de ligações telefônicas.

# Tipos de Phishing



## Smishing:

- Objetivo: solicitar dados pessoais por meio de mensagens de texto (SMS) ou aplicativos de mensagens instantâneas.
- Método: semelhante ao vishing, mas realizado via SMS ou aplicativos de mensagens.

## Phishing nas redes sociais:

- Objetivo: criar perfis falsos de empresas para enganar usuários.
- Método: compartilhar sorteios, descontos e ofertas falsas para interagir com as vítimas ou roubar suas informações por meio de links falsos

# Como os ataques de phishing funcionam?

Na maioria dos casos, começa com uma mensagem, sendo ela por e-mail, SMS, ligação ou até por redes sociais, influenciando o usuário a acessar um link, usando a mesma aparência do site original.

Ao acessar o link a vítima coloca suas informações pessoais. Com os dados dos usuários, os golpistas criam conta, fazem compras e fazem transferência de dinheiro. Pós ataque o cracker (nome referente a quem tem grandes níveis de conhecimento a tecnologia de informação) destrói quaisquer vestígios de desvio de dados. Dificultando possíveis investigações.



# Prevenção de ataques



- 1- Se receber e-mails pedindo informações pessoais ou financeira, não acesse ou entre no email ou no conteúdo. As organizações ou Contas Oficiais já sabem desse tipo de fraude não solicitam esses tipos de informações pelo e-mail, também não enviam SMS ou ligam. Outra alternativa é acessar o site oficial.
- 2- Se a criptografia ou assinatura digital não são usados, não envie informações pessoais pois não é um meio seguro de enviar informações
- 3- Não acessem suas contas em rede wifi públicos ou computadores públicos, os Pcs instalados nesses locais podem conter hardware ou softwares de más ações para capturar seus dados, os bancos oferecem teclado na tela.
- 4- Verifique se no canto esquerdo superior tem o cadeado fechado, note se o endereço web começa com https://

# Prevenção de ataques



- 5- Mantenha seu antivírus atualizado e os demais softwares, instale as atualizações de segurança do seu sistema operacional.
- 6- Não baixe ou abra arquivos de fontes desconhecidas. Podem conter softwares maliciosos que podem dar acesso ao seu computador e armazene seus dados pessoais
- 7- Olhe seu extrato de cartões, se você detectar cobranças ou pagamentos não autorizados, entre em contato com o banco imediatamente.
- 8- Não responder nenhuma mensagem suspeita, tal como um SMS de bem-vindo a um serviço que você não fez, exclua.

# Fontes

-[https://pagar.me/blog/o-que-e-phishing/?utm\\_source=google&utm\\_medium=cpc&utm\\_campaign=dsa&origin=search&media=google&type=pago&campaign=11366699401&ad\\_group=118179479464&ad=651857057688&theme=&gad\\_source=1&gclid=EAIalQobChMI-vDwl-vuhQMVCmNIAB1jjA5PEAAyASAAEgK59PD\\_BwE](https://pagar.me/blog/o-que-e-phishing/?utm_source=google&utm_medium=cpc&utm_campaign=dsa&origin=search&media=google&type=pago&campaign=11366699401&ad_group=118179479464&ad=651857057688&theme=&gad_source=1&gclid=EAIalQobChMI-vDwl-vuhQMVCmNIAB1jjA5PEAAyASAAEgK59PD_BwE)

[https://alura.com.br/artigos/entendendo-e-evitando-o-phishing?utm\\_term=&utm\\_campaign=%5BSearch%5D+%5BPerformance%5D+-+Dynamic+Search+Ads+-+Artigos+e+Conte%C3%BAdos&utm\\_source=adwords&utm\\_medium=ppc&hsa\\_acc=7964138385&hsa\\_cam=11384329873&hsa\\_grp=111087461203&hsa\\_ad=687448474447&hsa\\_src=g&hsa\\_tgt=dsa-1298415354460&hsa\\_kw=&hsa\\_mt=&hsa\\_net=adwords&hsa\\_ver=3&gad\\_source=1&gclid=EAIalQobChMlvN33jPruhQMVwUFIAB0cuQWpEAAYAyAAEgKEHPD\\_BwE](https://alura.com.br/artigos/entendendo-e-evitando-o-phishing?utm_term=&utm_campaign=%5BSearch%5D+%5BPerformance%5D+-+Dynamic+Search+Ads+-+Artigos+e+Conte%C3%BAdos&utm_source=adwords&utm_medium=ppc&hsa_acc=7964138385&hsa_cam=11384329873&hsa_grp=111087461203&hsa_ad=687448474447&hsa_src=g&hsa_tgt=dsa-1298415354460&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=EAIalQobChMlvN33jPruhQMVwUFIAB0cuQWpEAAYAyAAEgKEHPD_BwE)

<https://www.econo.unlp.edu.ar/detise/phishing-3923>