TIPOS DE PHISHING

PHISHING CLÁSSICO (OU TRADICIONAL)

- ENVIADO GERALMENTE POR E-MAIL EM MASSA, FINGINDO SER DE UMA EMPRESA LEGÍTIMA (BANCO, SERVIÇO ONLINE, ETC.).
- OBJETIVO: COLETAR DADOS COMO SENHAS E CARTÕES DE CRÉDITO VIA LINKS FRAUDULENTOS.

SPEAR PHISHING

- ATAQUES PERSONALIZADOS DIRECIONADOS A UMA PESSOA OU ORGANIZAÇÃO ESPECÍFICA.
- UTILIZA INFORMAÇÕES PESSOAIS PARA TORNAR A MENSAGEM MAIS CONVINCENTE.

VISHING (VOICE PHISHING)

- REALIZADO VIA LIGAÇÕES TELEFÔNICAS.
- OS CRIMINOSOS SE PASSAM POR ATENDENTES DE BANCO, SUPORTE TÉCNICO, POLÍCIA, ETC., PARA ROUBAR INFORMAÇÕES.

SMISHING (SMS PHISHING)

- MENSAGENS DE TEXTO (SMS) CONTENDO LINKS MALICIOSOS OU SOLICITAÇÕES DE DADOS SENSÍVEIS.

PHARMING

- REDIRECIONA O USUÁRIO A UM SITE FALSO, MESMO QUE ELE DIGITE CORRETAMENTE O ENDEREÇO VERDADEIRO.
- ENVOLVE MANIPULAÇÃO DE DNS OU DO PRÓPRIO DISPOSITIVO.

CLONE PHISHING

- UM E-MAIL LEGÍTIMO ANTERIOR É COPIADO E MODIFICADO PARA CONTER LINKS MALICIOSOS.
- ENVIADO A PARTIR DE UM ENDEREÇO SEMELHANTE AO ORIGINAL.

HQR CODE PHISHING (QUISHING)

- CÓDIGOS QR ADULTERADOS LEVAM A SITES MALICIOSOS, USADOS PRINCIPALMENTE EM CAMPANHAS FÍSICAS OU DIGITAIS.