S21 SEC

PHISHING

Cenários de ataque

Durante o primeiro semestre de 2020, os ataques de *phishing* foram um dos **principais riscos** para as empresas e utilizadores da internet.

Devido ao Coronavírus, os phishings converteram-se num dos ataques informáticos com mais êxito em todo o mundo

S21 SEC

Maior facilidade

Para realizar campanhas massivas de distribuição

+1000

Ataques de *Phishing* por mês

Aumento de 350%

Na criação de domínios maliciosos que se fazem passar por marcas e organizações

NOVAS ESTRATÉGIAS NOS ATAQUES DE *PHISHING*

Para empresas e instituições, os ataques de *phishing* constituem um risco duplo, impactando negativamente a sua imagem e atividade.

36% das empresas não têm claro se os seus colaboradores são capazes de detetar e evitar um ataque deste tipo.

38% das empresas reconhecem que foram vítimas deste tipo de ataques durante o último ano.

Este tipo de ataques realiza-se de forma cada vez mais profissional, com maior detalhe na redação, falsificação da identidade da marca ou criação de domínios

PRINCIPAIS SETORES afetados

Tecnológico

Financeiro

Redes sociais

24%

de *mail-phishing*

Está centrado em Microsoft, Outlook e Unicredit

FALSIFICAÇÃO DE IDENTIDADE

nos ataques de *phishing*

Realiza-se maioritariamente no Google, Amazon, WhatsApp e Facebook

61%

dos ataques Web

envolveram a Google, WhatsApp e Facebook

21:00h

PHISHING móveis

Uma nova realidade

Os ataques de *phishing* em dispositivos móveis aumentaram 37% em 2020

A deteção de links fraudulentos é mais difícil de detetar pelos utilizadores nos dispositivos móveis.

Supermercados

Transportadoras

Instituições Públicas

Banco

EMPRESAS MAIS AFETADAS

Promoções e Descontos

Confirmação de informações pessoais

Ofertas

Reativação de dispositivos

ISCOS MAIS USADOS

Email

SMS

Chamadas de voz

Apps de mensagens

Apps de Redes Sociais

NOVOS RISCOS

Utilizadores

Colaboradores

TARGET AMPLIADO

APPS MAIS AFETADAS

PHISHING na era do COVID-19

GOOGLE

Confirmou que dos 100 milhões de emails de *phishing* bloqueados pelo Gmail, 18 milhões estavam relacionados com a pandemia.

AMAZON

Foi classificada a empresa que mais sofreu de falsificação de identidade durante os meses de confinamento. Ataques de *phishing* dirigidos a utilizadores que efetuaram compras através da plataforma.

OMS

Reportou um crescimento deste tipo de ataques que falsificavam a sua imagem e a de colaboradores da organização para enganar os utilizadores e empresas por todo o mundo em diferentes campanhas.

CIBERSEGURANÇA

Na S21Sec registámos um aumento deste tipo de ataques desde o início da pandemia, observando um crescimento de 53%.

A S21SEC OBSERVOU UM CRESCIMENTO EXPONENCIAL NO ROUBO DE INDENTIDADE DE INSTITUIÇÕES PÚBLICAS EM CAMPANHAS DE *PHISHING*

Os atacantes usam a imagem de instituições públicas para fins ilegais.

Operações de distribuição de código malicioso.

Campanhas de roubo de credenciais.

- Um em cada três incidentes de segurança envolveu previamente um ataque de *phishing*.
- A Europa é a primeira região do mundo na receção de *phishing* e emails com conteúdo malicioso.
- Durante o segundo trimestre de 2020, Espanha, Rússia e Alemanha somam um total 22,75% do total de ataques mundiais com e-mails com anexos maliciosos ou links para sites de *phishing*.
- As campanhas de *phishing* e distribuição de malware atuam cada vez mais de forma interrelacionada.

PENSE ANTES DE CLICAR

Nuca abra um anexo ou clique num link de remetentes não identificados.

NÃO CONFIE

Em promoções, ofertas ou sorteios. Comprove sempre as páginas oficiais das empresas.

VERIFIQUE A FONTE

Especialmente se o email pede confirmação de informação pessoal ou financeira.

MANTENHA MEDIDAS

Atualize as suas passwords periodicamente.

INSTALE SOLUÇÕES

De segurança nos seus dispositivos e mantenha-as atualizadas.

S21 SEC

www.s21sec.com
marketing@s21sec.com