CAMPANHA *ANTI-PHISHING* NA CAPES

CAMPANHA *ANTI-PHISHING* NA CAPES

Nas últimas semanas, a Diretoria de Tecnologia da Informação - DTI enviou aos usuários da Capes, dois e-mails falsos simulando um ataque externo para avaliar a atenção e conhecimento das boas práticas de segurança da informação dos usuários, referente à e-mails ou ataques maliciosos.

CAMPANHA *ANTI-PHISHING* - WEBMAIL

Durante a campanha “Webmail”, a DTI enviou cerca de 1254 e-mails simulando tentativas e-mails maliciosos, cujo assunto era a implementação de melhorias e novas funcionalidades no webmail da CAPES, solicitando o usuário a clicar em um link para explorar os recursos e benefícios do software.


ter 30/03/2021 11:28
Diretoria de Tecnologia da Informação <bouncer62612048.mailer@gmail.com>
[Aviso DTI] Novas funcionalidades no Webmail
Para [redacted]
Você encaminhou esta mensagem em 30/03/2021 11:31.
Clique aqui para baixar imagens. Para ajudar a proteger sua privacidade, o Outlook impediu o download automático de algumas imagens desta mensagem.

Webmail - Novas Funcionalidades

Prezado(a) Servidor/Colaborador,

O sistema Webmail da CAPES está com um novo visual, com novas funcionalidades e algumas melhorias.

A atualização traz benefícios como: pesquisa mais rápida, calendário com novo layout, preenchimento automático para resposta, entre outros.

Acesse https://webmail.capes.gov.br/novidades parar explorar os novos recursos.

Equipe DTI

Figura 1 - E-mail de simulação de ataque malicioso - Campanha Anti-Phishing "Webmail"

Durante a campanha “Webmail”, a DTI enviou cerca de 1254 e-mails simulando tentativas e-mails maliciosos, cujo assunto era a implementação de melhorias e novas funcionalidades no webmail da CAPES, solicitando o usuário a clicar em um link para explorar os recursos e benefícios do software.

Em análise dos resultados, a DTI identificou que que 10,05% dos usuários clicaram no link falso, 7,26% enviaram seu usuário/senha e menos de 1% reportou à DTI sobre o e-mail suspeito recebido.

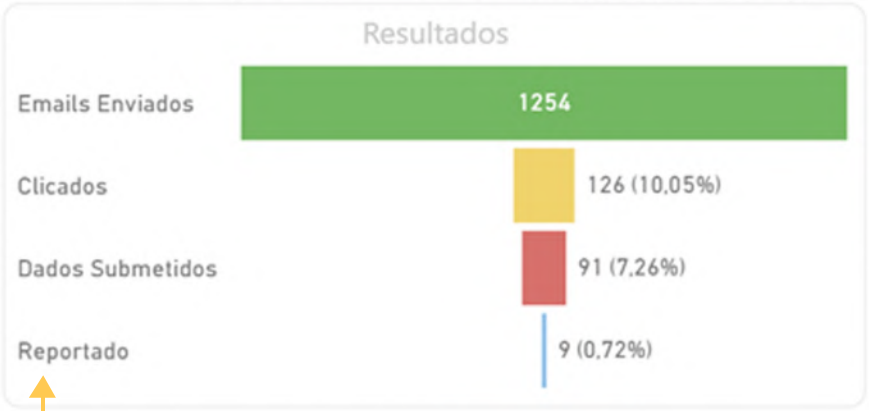

Figura 2 - Resultado da Campanha Anti-Phishing "Webmail"

CAMPANHA DE ANTI-PHISHING BANCO - INVESTIMENTO

Já a campanha "Banco – Investimento", simulava um e-mail bancário e continha um link falso que incentivava o usuário a clicar em "descadastrar" com intuito de não mais receber supostas futuras mensagens de marketing deste banco.

Figura 3 - E-mail de simulação de ataque malicioso - Campanha "Banco – Investimento"

Os resultados mostraram que 2,23% dos usuários clicaram no link falso e 0,24% reportaram à DTI sobre o e-mail suspeito recebido. O baixo percentual de “Clicados” possivelmente se deu pela ação dos usuários de excluir e/ou ignorar o e-mail.

Figura 4 Resultado da Campanha de Anti-Phishing – “Banco - Investimento”

ENTENDA MAIS SOBRE O GRAU DESTE TIPO DE AMEAÇA E COMO IDENTIFICÁ-LAS.

Normalmente, não é uma tarefa simples atacar sistemas computacionais de uma instituição e, por este motivo, golpistas focam esforços na exploração de fragilidades dos usuários. Usando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir os potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar sites falsos. Um destes ataques é o phishing.

O QUE É PHISHING?

O termo phishing faz alusão à palavra em inglês fishing, que significa "pescaria". A associação com essa atividade não é mero acaso: o phishing scam ou apenas phishing é uma tentativa de fraude pela Internet que utiliza "iscas", isto é, artifícios para atrair a atenção de um usuário e fazê-lo realizar alguma ação.
Caso o usuário se torne vítima do golpe poderá acabar informando dados sensíveis ou outras informações confidenciais ao atacante, percebendo tardiamente que foi vítima de uma fraude. Da mesma forma, poderá contaminar o seu computador ou smartphone com um código malicioso.

SPAM X PHISHING

A principal diferença entre spam e phishing é que os spammers não querem prejudicar você. Spam é lixo eletrônico: apenas um monte de anúncios indesejados. Os golpes de phishing têm como objetivo roubar seus dados e usá-los contra você.

VOCÊ SABIA?

"O primeiro caso de phishing conhecido foi registrado judicialmente em 2004, quando um adolescente da Califórnia criou um site falso e passou a obter informações confidenciais dos usuários. Com os dados obtidos, o jovem passou a retirar dinheiro das contas."

COMO FUNCIONA?

Os crimes de phishing podem chegar até você via email, SMS, ligações telefônicas, falsos sites e falsos pop-ups inseridos em sites desprotegidos, todos com uma abordagem atrativa. Os conteúdos podem ser dos mais variados, em nome de bancos, governo, instituições financeiras, como PayPal ou até mesmo Correios, sempre solicitando uma ação ou informação. Por exemplo, pode ser pedido para que abra determinado link ou arquivo, faça ligação ou instale/atualize um software específico. Os criminosos utilizam de todas as formas para atacar os usuários e conseguir acesso à informações sigilosas das quais poderão se beneficiar

ESTATÍSTICAS

O ano de 2020 foi marcado pela pandemia e, consequentemente, pela transição massiva para o teletrabalho e comunicações online. Tudo isto se refletiu nas estatísticas de ataques por spam e phishing em todo o mundo. Segundo a Kaspersky, Portugal foi um dos países que mais sofreu com este tipo de ciberataque, aparecendo em segundo lugar no top dos 10 países com mais vítimas de phishing, a nível global.

Segundo o mais recente relatório da Kaspersky, em 2020 foram identificados cerca de 430 milhões de tentativas de ataques de phishing, sendo que o Brasil volta a liderar a tabela dos países com maior número de vítimas afetadas (19,94%), logo seguido de Portugal, que se apresenta em segundo lugar com 19,73% do total de ataques, a nível mundial. Contudo, os indicadores de ambos os países baixaram, relativamente ao ano de 2019. Neste período, o Brasil apresentava mais 10 pontos percentuais e Portugal mais 6.

O relatório mostra ainda que França – que não aparecia no top 10 desde 2015 – atingiu o terceiro lugar (17,90%) e que a Venezuela, o país líder em 2019 (e que liderou também o ranking nos dois primeiros trimestres de 2020), caiu para oitavo lugar.

Esta é a lista dos 10 países mais afetados por ataques de phishing:

- Brasil: **19,94%**
- França: **17,90%**
- Guiana Francesa: **17,60%**
- Camarões: **17,32%**
- Nepal: **16,72%**
- Portugal: **19,73%**
- Tunísia: **17,62%**
- Catar: **17,35%**
- Venezuela: **16,84%**
- Austrália: **16,59%**

NO BRASIL...

Em 2020, o Brasil foi o país mais atingido por tentativas de roubo de dados pessoais ou financeiros de pessoas na internet, prática denominada em inglês de phishing. Com essas informações, golpistas prejudicam a vítima de diversas formas, seja acessando recursos ou enganando pessoas se fazendo passar por ela.

De acordo com a companhia, entre fevereiro e março do ano passado, o número de ataques cresceu 120% no Brasil.

Os golpes foram aplicados por meio de links em mensagens ou sites falsos, que se passam por empreendimentos conhecidos, como grandes cadeias de varejo online - Amazon e outras.

Os exemplos mais comuns foram golpes em que os criminosos enviaram mensagens se passando por essas lojas e pedindo para a vítima contatar as áreas de comunicação com o cliente ou de suporte, com sistemas para roubar dados dos usuários acionados.

Aplicativos de comunicação, especialmente o Whatsapp, tornaram-se os principais canais para aplicar esses golpes. Usuários receberam mensagens com promessas de prêmios com links que levavam a sites falsos destinados a roubar informações da vítima.

NO BRASIL...

Na prática, veja como você pode identificar possíveis ameaças:

- Verificar e analisar o endereço de e-mail dos remetentes;
- Não compartilha informações pessoais através de redes sociais;
- Evitar abrir um anexo que vem em um e-mail não solicitado;
- Não responda ou clique em links em e-mails que peçam informações pessoais, financeiras ou de contas;
- Verifique os cabeçalhos e assuntos das mensagens;
- Em caso de dúvida sempre procure o suporte técnico de TIC através dos canais 2022-6170 - cati@capes.gov.br

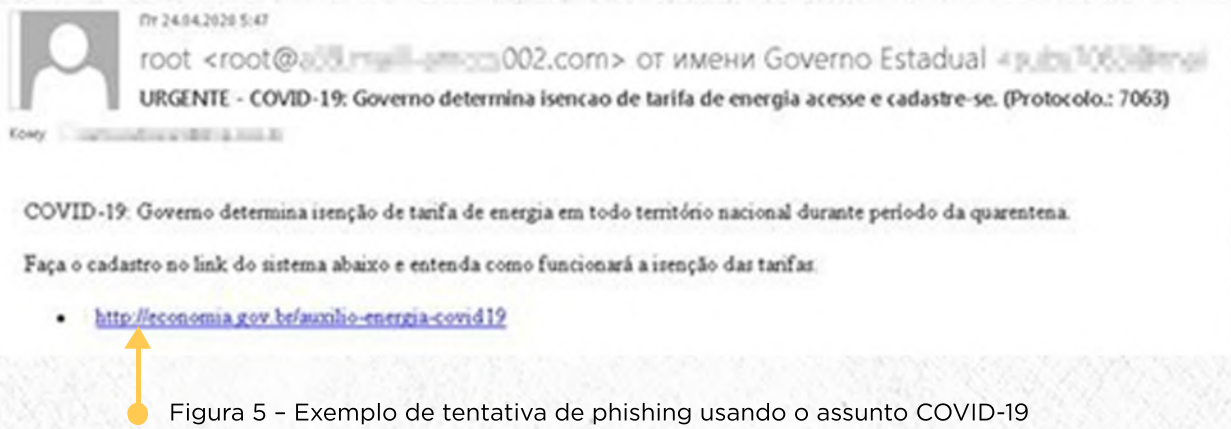

Figura 5 – Exemplo de tentativa de phishing usando o assunto COVID-19

FONTES

[1]https://www.ic3.gov/Home/AnnualReports

[2]https://thehill.com/policy/cybersecurity/504389-fbi-sees-major-spike-in-coronavirus-related-cyber-threats

[3]https://www.europol.europa.eu/newsroom/news/europol-publishes-law-enforcement-and-industry-report-spear-phishing

[4]https://securelist.com/spam-and-phishing-in-2020/100512/

[5]https://www.kaspersky.com.br/blog/covid-compensation-spam/1555

[6]https://www.infowester.com/phishing.php

https://gatefy.com/pt-br/blog/o-que-e-phishing/

https://cartilha.cert.br/golpes/

https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet

https://www.avast.com/pt-br/c-phishing

https://agenciabrasil.ebc.com.br/geral/noticia/2021-03/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet#:~:text=Em%202020%2C%20o%20Brasil%20foi,denominada%20em%20ingl%C3%AAs%20de%20phishing.&text=O%20percentual%20de%20usu%C3%A1rios%20brasileiros,9%25%20dos%20internautas%20do%20pa%C3%ADs.

https://www.computerworld.com.pt/2021/03/15/portugal-e-o-segundo-pais-do-mundo-com-mais-vitimas-de-phishing/#:~:text=a%20n%C3%ADvel%20global.-,Segundo%20o%20mais%20recente%20relat%C3%B3rio%20da%20Kaspersky%2C%20em%202020%20foram,19%2C73%25%20do%20total%20de