Insights sobre phishing 2021

Embora o phishing já exista há um quarto de século, ele continua sendo uma técnica de ataque cibernético eficaz especialmente porque evolui continuamente. Os invasores são rápidos em identificar novas oportunidades de phishing – muitas proporcionadas pela pandemia – e desenvolver novas táticas e técnicas.

Para as organizações, o phishing costuma ser a primeira etapa de um ataque complexo em vários estágios. Os invasores costumam usar o phishing para induzir os usuários a instalem malware ou compartilhem credenciais que concedem acesso à rede da vítima. Um e-mail aparentemente inócuo pode levar a ransomware, criptojacking ou roubo de dados.

Este documento apresenta os insights mais recentes sobre phishing com base em uma pesquisa independente com 5.400 profissionais de TI da linha de frente em todo o mundo, juntamente com um estudo de caso de um ataque real de phishing que levou a um incidente multimilionário de ransomware.

De acordo com o Data Breach Investigation Report de 2021 da Verizon, 36% das violações de dados confirmadas envolvem phishing (em comparação a 25% em 2019). Use os resultados da pesquisa para avaliar sua própria postura de segurança contra phishing e identificar oportunidades para ampliar sua proteção.

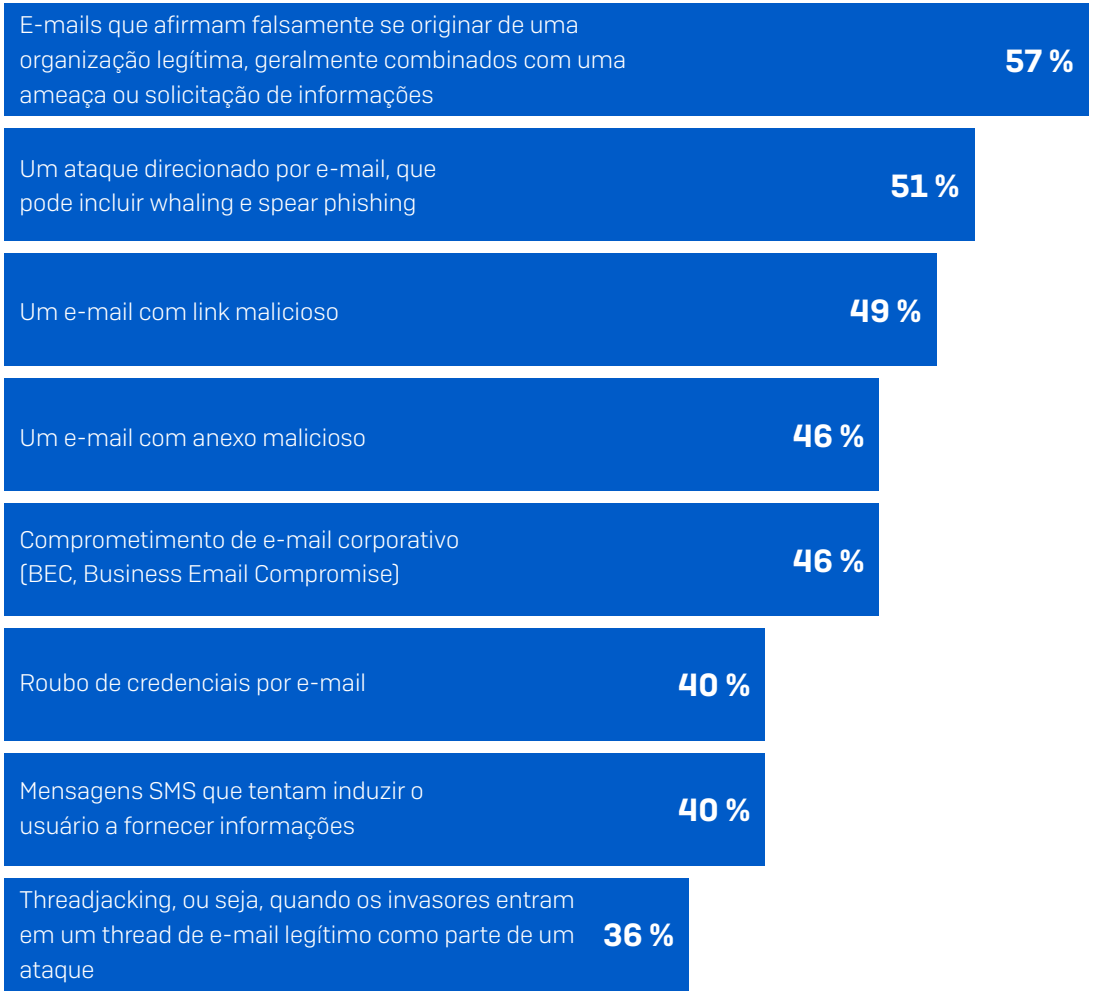
SOPHOS

1. Phishing tem diferentes significados para diferentes pessoas

O que é phishing? A pesquisa revela que, mesmo entre os profissionais de TI, há uma grande variação no entendimento das pessoas sobre o que consideram um ataque de phishing. O entendimento mais comum é que se trata de *e-mails que afirmam falsamente se originar de uma organização legítima, geralmente combinados com uma ameaça ou solicitação de informações*. Embora essa seja a resposta mais popular, menos de seis em cada 10 (57%) respondentes selecionaram essa opção, ilustrando a ampla gama de significados dados ao phishing.

46% dos respondentes consideram os ataques de comprometimento de e-mail corporativo (BEC, Business Email Compromise) como phishing, enquanto mais de um terço (36%) entende que o threadjacking, ou seja, quando os invasores se inserem em uma conversa legítima de e-mails como parte de um ataque, também deve ser considerado phishing.

Qual das seguintes opções você considera um ataque de phishing?



Qual destas opções você considera um ataque de phishing? [5.400] Excluindo algumas opções de resposta

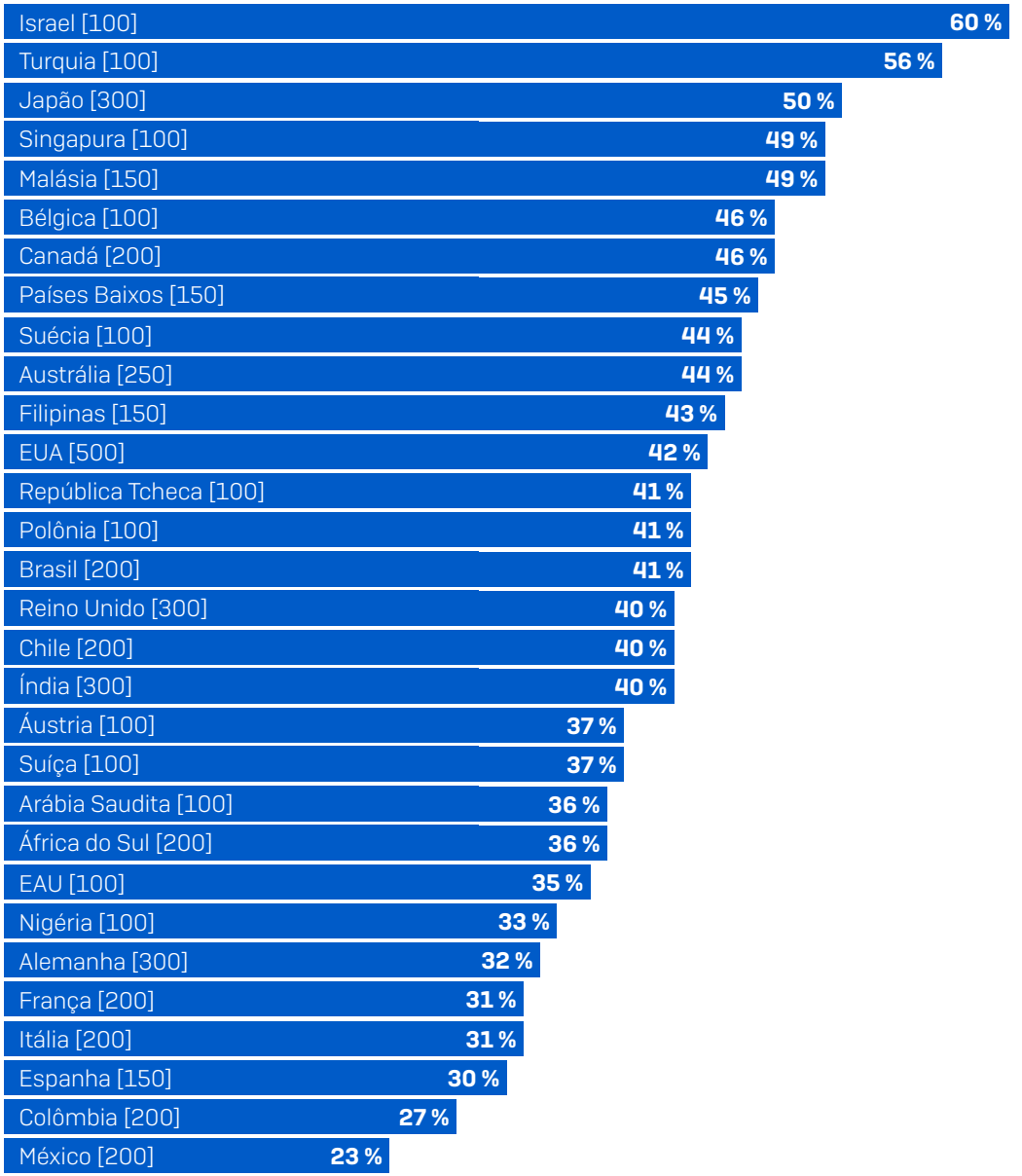
Fatores culturais têm um grande impacto na compreensão das pessoas sobre o que é phishing. Por exemplo, a proporção de respondentes em Israel que considera phishing as mensagens SMS que tentam induzir o usuário a fornecer informações é mais do que o dobro da porcentagem no México (60% contra 23%). Embora muitos profissionais de TI chamem isso de smishing em vez de phishing, mensagens falsas alegando ser de marcas em que confiamos têm o mesmo efeito, independentemente do método de transmissão.

Considerando essa ampla variação entre os profissionais de TI sobre como eles entendem ou definem os ataques de phishing, é razoável esperar uma gama semelhante ou maior de interpretações entre os funcionários que não são de TI.

Entender que phishing tem diferentes significados para diferentes pessoas é importante para qualquer pessoa que crie ou execute programas educacionais e de conscientização sobre phishing. Para que o treinamento sobre phishing seja eficaz, é importante garantir uma definição de referência compartilhada de phishing para que o conceito que aprendemos seja compreendido no contexto correto.

CONCLUSÃO: ESTEJA CIENTE DE QUE PHISHING TEM DIFERENTES SIGNIFICADOS PARA DIFERENTES PESSOAS QUANDO FORNECER RECURSOS EDUCACIONAIS E DE TREINAMENTO DE CONSCIENTIZAÇÃO DO USUÁRIO. SEM O CONTEXTO CORRETO, O TREINAMENTO NÃO SERÁ TÃO EFICAZ.

Respondentes que consideram mensagens SMS que tentam induzir o usuário a fornecer informações como phishing



Qual destas opções você considera um ataque de phishing? [números de base no gráfico] Mensagens SMS que tentam induzir o usuário a fornecer informações

2. A incidência de phishing aumentou consideravelmente desde o início da pandemia

70% dos respondentes relataram um aumento nos ataques de phishing em suas organizações desde o início da pandemia. Todos os setores foram afetados, sendo que o governo central enfrentou o maior aumento (77%), seguido de perto por empresas e serviços profissionais (76%) e saúde (73%).

A pequena variação entre setores – apenas 10 pontos percentuais antes do arredondamento* – afirma que os invasores não costumam discriminar e tentam atingir o máximo possível de pessoas para aumentar a probabilidade de sucesso.

A pesquisa do SophosLabs mostrou que os invasores foram rápidos em aproveitar as oportunidades apresentadas pela pandemia e a resultante indefinição dos limites centre casa e trabalho, incluindo:

- Aumento rápido do trabalho em casa. Os invasores provavelmente esperavam que as pessoas baixassem a guarda enquanto se ajustavam ao trabalho em casa e às operações em um ambiente não comercial.
- Crescimento nas entregas a domicílio. Mensagens de phishing que pareciam ser de uma empresa de entrega a domicílio tornaram-se comuns nos primeiros meses da pandemia, à medida que as pessoas passaram a fazer muitas compras online.
- Preocupação generalizada com a pandemia. Os invasores exploraram a ansiedade e a necessidade de informações das pessoas sobre a COVID-19 para aplicar golpes relacionados à pandemia. Eles previram que o alto nível de preocupação tornaria as pessoas menos propensas a verificar a legitimidade de uma mensagem antes de clicar.

Setor	Os respondentes que enfrentaram um aumento nos ataques de phishing em suas organizações desde o início da pandemia
Governo central e NDPB [117]	77 %
Serviços profissionais e empresariais [361]	76 %
Saúde [328]	73 %
Mídia, lazer e entretenimento [145]	72 %
Energia, petróleo/gás e serviços de utilidade [197]	72 %
Varejo [435]	71 %
Educação [499]	71 %
Outros [768]	71 %
Governo local [131]	69 %
Distribuição e transporte [203]	68 %
Serviços financeiros [550]	68 %
Construção civil [232]	68 %
TI, tecnologia e telecomunicações [996]	68 %
Manufatura e produção [438]	66 %

Você percebeu um aumento nos ataques de que o número de phishing em sua organização desde o início da pandemia? [números de base no gráfico] Sim, um grande aumento, Sim, um aumento pequeno

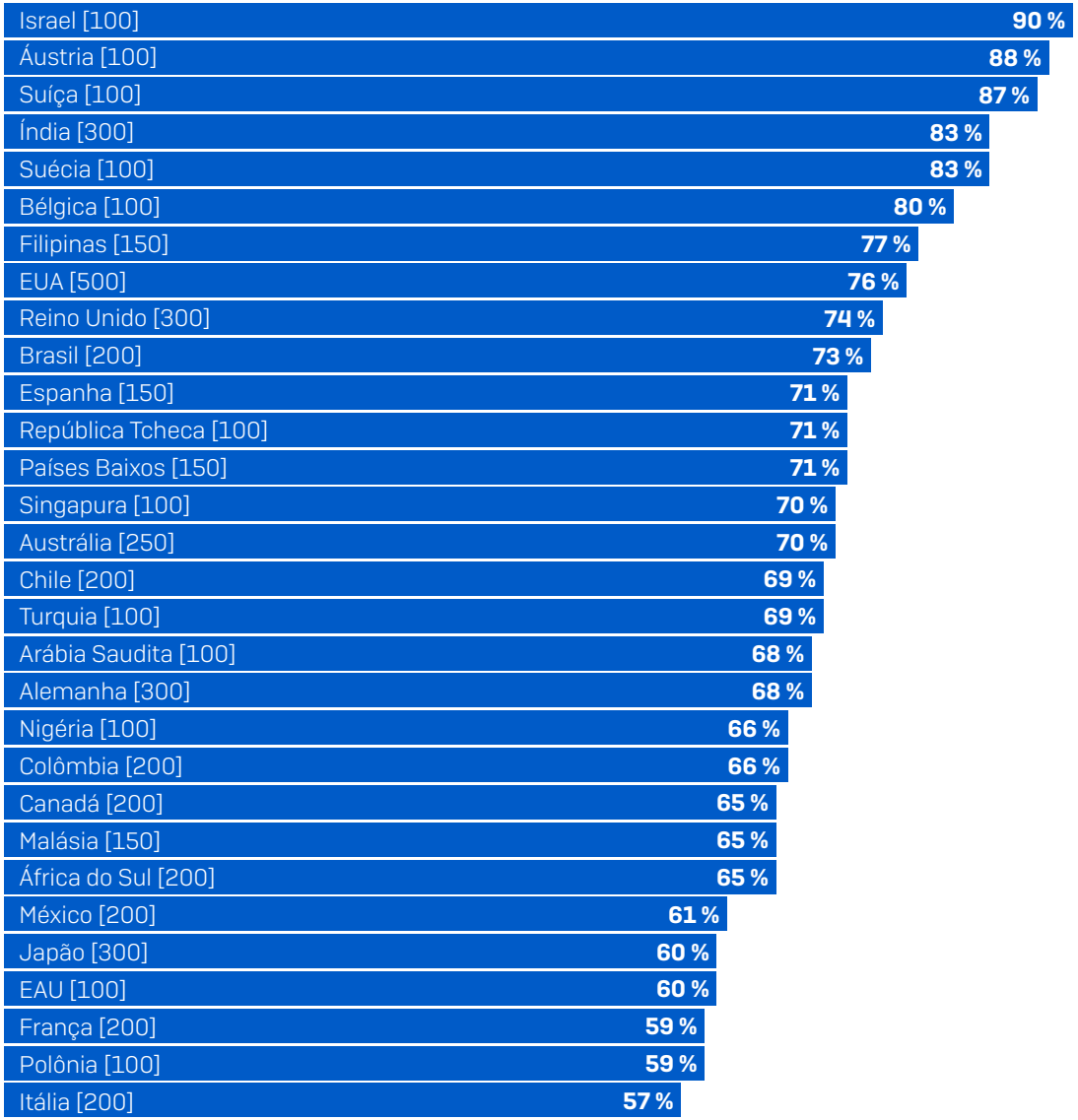
** Antes do arredondamento, 76,92% dos respondentes no governo central relataram um aumento em comparação com 66,43% na indústria, resultando em uma variação real de 10,48%*

Apesar da pouca variação geral por setor, a pesquisa revelou uma diferença considerável no aumento de ataques de phishing relatados por país desde o início da pandemia. Por exemplo, 90% dos respondentes em Israel relataram um aumento no phishing em comparação com 57% na Itália. Esses resultados, embora influenciados pela definição de phishing dos respondentes e sua capacidade de rastrear e mensurar os ataques, oferecem um insight valioso sobre a experiência real dos profissionais de TI na linha de frente.

Assim como há vários tipos diferentes de e-mails de phishing, também existem diferentes criminosos cibernéticos por trás deles. Grupos de invasores habilidosos normalmente concentram seus ataques direcionados em países com PIB mais alto, como Áustria, Suíça e Suécia, para maximizar seu retorno financeiro, o que provavelmente contribuiu para o aumento generalizado de phishing nesses países. Ao mesmo tempo, o phishing também é usado em ataques do tipo "spray and pray" em massa, em que os invasores esperam que, se tentarem uma quantidade suficiente de pessoas, alguém acabará sendo vítima do golpe.

CONCLUSÃO: NÃO DESISTA DE SEUS ESFORÇOS ANTI-PHISHING. OS CRIMINOSOS CIBERNÉTICOS ESTÃO INTENSIFICANDO O USO DESSA TÉCNICA SEM POUPAR NENHUM SETOR OU PAÍS.

Respondentes que enfrentaram um aumento no número de ataques de phishing em suas organizações desde o início da pandemia



Você percebeu um aumento nos ataques de que o número de phishing em sua organização desde o início da pandemia? [números de base no gráfico] Sim, um grande aumento, Sim, um aumento pequeno

3. A maioria das organizações realiza programas de conscientização sobre segurança cibernética para lidar com o phishing

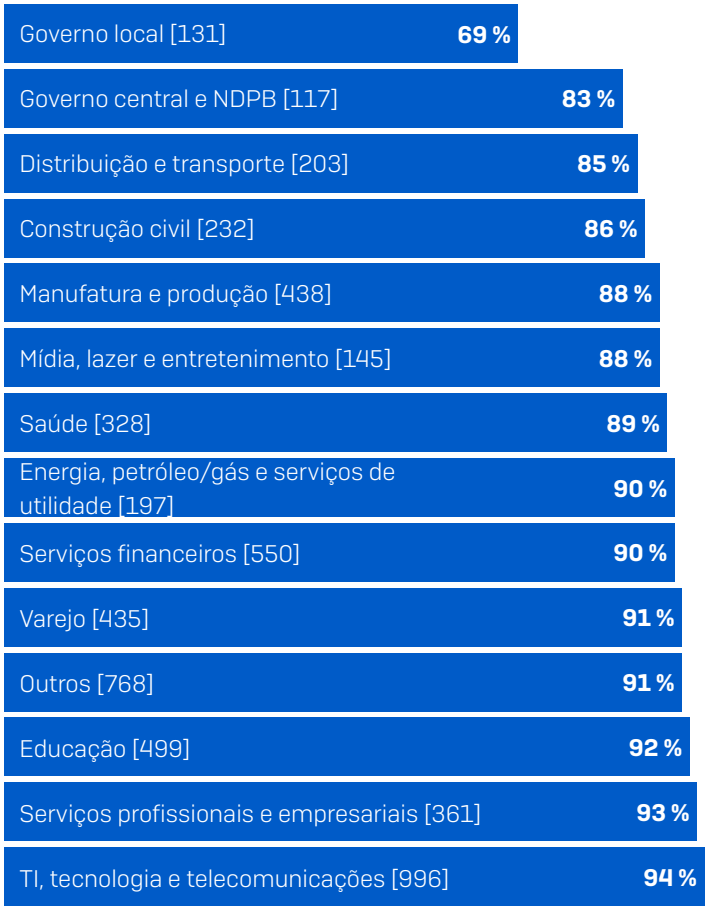
90% das organizações implementaram um programa de conscientização cibernética para lidar com phishing, com mais 6% planejando implementar um programa desse tipo.

A abordagem mais popular é o treinamento baseado em computador, usado por 58% das organizações. Mais da metade (53%) usa treinamento ministrado por instrutor e 43% executa simulações de phishing. 16% das organizações combinam as três técnicas em seus programas de conscientização: treinamento baseado em computador, treinamento ministrado por instrutor e simulações de phishing.

A pesquisa revelou que o setor governamental fica para trás quanto à realização de programas de conscientização sobre segurança cibernética para lidar com o phishing, com os dois últimos pontos alocados ao governo local (69%) e governo central (83%). Trata-se de uma situação preocupante, pois as organizações governamentais são alvos frequentes de ataques cibernéticos de alto impacto: o governo central tem maior probabilidade de sofrer ataques de ransomware no estilo extorsão, enquanto o governo local tem maior probabilidade de ter seus dados criptografados em um ataque de ransomware.

CONCLUSÃO: SE VOCÊ ESTIVER ENTRE OS 10% QUE AINDA NÃO TÊM UM PROGRAMA DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA CIBERNÉTICA PARA LIDAR COM PHISHING, IMPLEMENTE UM IMEDIATAMENTE.

Uso de programas de conscientização sobre segurança cibernética para lidar com o phishing



A sua organização tem um programa de conscientização sobre segurança cibernética para lidar com phishing? [5.400] Sim, realizamos programas de treinamento baseados em computador; Sim, realizamos programas de treinamento ministrados por instrutores; Sim, fazemos simulações de phishing

90%

implementaram um programa de conscientização cibernética para lidar com phishing

58%

realizam programas de treinamento baseados em computador

53%

realizam programas de treinamento ministrados por instrutores

43%

realizam simulações de phishing

A sua organização tem um programa de conscientização sobre segurança cibernética para lidar com phishing? [5.400] Sim, realizamos programas de treinamento baseados em computador; Sim, realizamos programas de treinamento ministrados por instrutores; Sim, fazemos simulações de phishing

4. Os programas de conscientização sobre phishing estão bem estabelecidos

Quase dois terços (65%) dos programas de conscientização sobre phishing foram implementados entre um e três anos atrás, refletindo a resposta das organizações à mudança na técnica dos invasores em meados da última década. As melhorias nas defesas cibernéticas contra ataques baseados na Web em meados da década de 2010 forçaram os invasores a mudarem para novos vetores, como e-mail, criando a forte necessidade de programas de educação do usuário.

Considerando o aumento generalizado de phishing desde o início da pandemia, é encorajador que 98% das organizações tivessem um programa de conscientização sobre phishing em vigor antes da COVID-19. Graças a esses programas, os funcionários estavam bem posicionados para resistir à enxurrada de e-mails de phishing no ano passado.

CONCLUSÃO: CERTIFIQUE-SE DE REVISAR E ATUALIZAR REGULARMENTE SEUS MATERIAIS E ATIVIDADES DE CONSCIENTIZAÇÃO SOBRE PHISHING PARA GARANTIR QUE ELES CONTINUEM RELEVANTES E ENVOLVENTES PARA OS USUÁRIOS.

Quando sua organização implementou o programa de conscientização sobre segurança cibernética para lidar com phishing?	
No último ano	2 %
Há 1 ou 2 anos	30 %
Há 2 ou 3 anos	35 %
Há 3 ou 4 anos	20 %
Há 4 ou 5 anos	12 %
Há mais de 5 anos	0 %
Não sabe	1 %

Respondentes cuja organização tem um programa de conscientização em vigor para lidar com phishing [4.866]

5. Medidas positivas de rastreamento dominam a avaliação da eficácia do treinamento

Quase todas (98%) as organizações que implementam um programa de conscientização do usuário para lidar com phishing avaliam o impacto de seus esforços. Mensurar e acompanhar os resultados permite que as organizações otimizem seus programas para melhorar os resultados.

As abordagens mais comuns são acompanhar o número de e-mails de phishing relatados à TI (68%) e/ou o nível de relatos de phishing feitos pelos usuários (65%). É animador que essas medidas construtivas que refletem boa consciência e comportamento positivo do usuário sejam as mais comuns. Identificar e aumentar a conscientização sobre phishing permite que as equipes de TI evitem proativamente que outras pessoas se tornem vítimas de golpes.

Metade das organizações (50%) rastreia a taxa de cliques em e-mails de phishing. Embora seja uma medida negativa (focada em ser vítima do golpe), a taxa de cliques fornece às equipes de TI dados para ajudá-las a direcionar os programas de conscientização para setores em que eles são mais necessários e a adaptar o conteúdo para refletir a realidade da organização. Quanto mais pontos de dados, positivos e negativos, você rastrear, melhor.

CONCLUSÃO: REVISE REGULARMENTE SEUS PROGRAMAS DE EDUCAÇÃO DO USUÁRIO À LUZ DOS RESULTADOS DE SUAS AVALIAÇÕES E CONCENTRANDO-SE EM RECONHECER E COMEMORAR COMPORTAMENTOS POSITIVOS.

98% avaliam o impacto de seu programa de conscientização

68% Rastreiam o número de tíquetes relacionados a phishing encaminhados à TI

65% Rastreiam o nível de relatos de e-mails de phishing feitos pelos usuários

50% Rastreiam a taxa de cliques em e-mails de phishing

O que você rastreia para avaliar o impacto do seu programa de conscientização? [4.866 respondentes cuja organização tem um programa de conscientização em vigor para lidar com phishing] Número de tíquetes relacionados a phishing encaminhados à TI; Nível de relatos de e-mails de phishing feitos pelos usuários; Taxa de cliques em e-mails de phishing. Não avaliamos o impacto de nossos programas de conscientização sobre phishing. Exclui algumas opções de resposta

Estudo de caso: Como um e-mail de phishing levou a um ataque multimilionário de ransomware

A equipe do Sophos Rapid Response foi recentemente chamada para ajudar uma empresa que estava enfrentando um grande ataque de ransomware. Depois que o ataque foi contido, a equipe do Rapid Response investigou o incidente para entender como ele começou. A equipe descobriu que:

Três meses antes do ataque, um funcionário recebeu um e-mail de phishing. O e-mail parecia ser de um colega em outro escritório. Provavelmente, os invasores acessaram a conta de e-mail do funcionário para levar os colegas de trabalho a confiarem na mensagem.

A mensagem, que era muito breve e mal redigida, solicitava que o funcionário clicasse em um link para conferir um documento. Na verdade, tratava-se de um link malicioso e, quando o funcionário clicou nele, os invasores obtiveram as credenciais de acesso do administrador do domínio.

A equipe do Rapid Response acredita que o e-mail de phishing foi enviado por um agente de acesso inicial (Initial Access Broker), um criminoso cibernético que se concentra em proteger o acesso aos ambientes das organizações para depois vender o acesso a outros invasores para uso em uma série de ataques, incluindo ransomware e roubo de dados.

Nesse caso, a equipe de TI da vítima interveio e encerrou o ataque de phishing. Isso parecia ser o final da história.

Porém, oito semanas depois, um agente malicioso instalou e executou duas ferramentas no computador da vítima: Cobalt Strike e PowerSploit PowerView. Tratam-se de ferramentas comerciais usadas legitimamente por testadores de invasão, mas também por criminosos cibernéticos para fins maliciosos. Os invasores provavelmente usaram o PowerView para fazer o reconhecimento da rede, enquanto o Cobalt Strike forneceu persistência, permitindo a permanência na rede.

Após a atividade exploratória dos invasores, não houve atividades por cerca de duas semanas. A equipe do Rapid Response acredita que isso ocorreu porque o agente de acesso inicial estava procurando um comprador ideal para as credenciais de acesso.

Depois da venda, os novos "proprietários" foram rápidos em aproveitar sua compra. Em pouco tempo eles apareceram na rede, instalaram o Cobalt Strike em mais máquinas e começaram a coletar e roubar informações.

Três meses após o e-mail de phishing original, os invasores lançaram o ransomware REvil às 4 horas da manhã, horário local, e exigiram um resgate de US$ 2,5 milhões.

Obtenha proteção contra phishing com tecnologia de IA com o Sophos Email

O machine learning avançado **identifica impostores de phishing e ataques BEC**

A verificação em tempo real dos principais indicadores de phishing **bloqueia técnicas de engenharia social**

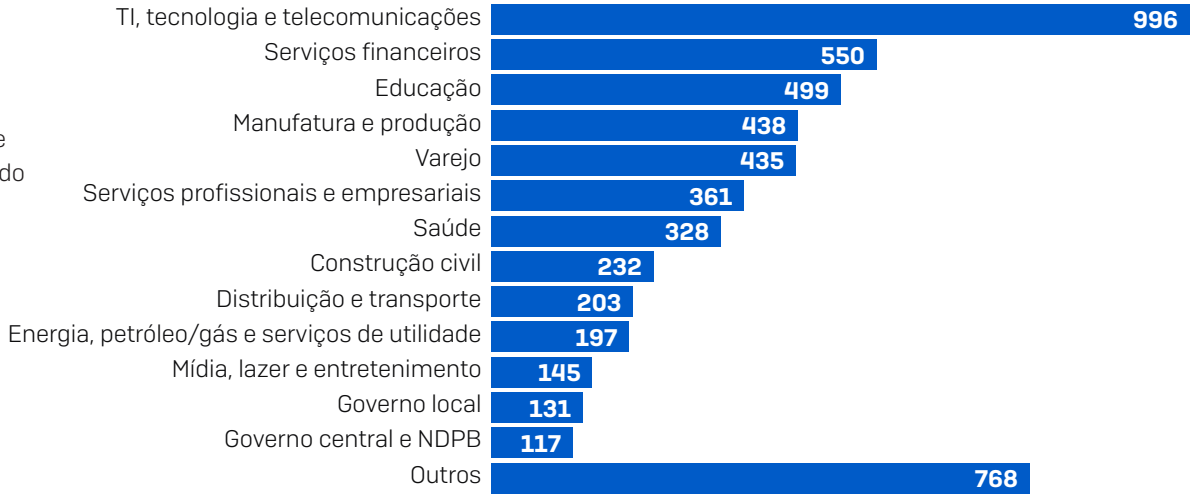
A proteção anterior e posterior à entrega bloqueia **links maliciosos e malware**

Saiba mais e experimente gratuitamente em sophos.com/email

Sobre a pesquisa

A Sophos contratou uma empresa independente de pesquisa de opinião, a Vanson Bourne, para consultar 5.400 tomadores de decisão de TI em organizações de médio porte (100 a 5.000 funcionários) em 30 países. A pesquisa foi conduzida em janeiro e fevereiro de 2021. Os respondentes pertenciam aos setores privado e governamental/público.

Número de respondentes por setor



Número de respondentes por país

País	Nº de respondentes	País	Nº de respondentes	País	Nº de respondentes
Austrália	250	Índia	300	Arábia Saudita	100
Áustria	100	Israel	100	Singapura	150
Bélgica	100	Itália	200	África do Sul	200
Brasil	200	Japão	300	Espanha	150
Canadá	200	Malásia	150	Suécia	100
Chile	200	México	200	Suíça	100
Colômbia	200	Países Baixos	150	Turquia	100
República Tcheca	100	Nigéria	100	EAU	100
França	200	Filipinas	150	Reino Unido	300
Alemanha	300	Polônia	100	EUA	500

2021-08-13 WPEN (NP)

SOPHOS