

Resultado do 1º ciclo da campanha de *phishing* do **RIOPREVIDÊNCIA**



Elaboração deste documento

Gerência de Tecnologia da Informação e Comunicação
Coordenadoria DPO

1 Campanha de *phishing*



1.1 Treinamentos

Entre os dias **03 e 14 de junho de 2024**, ocorreu um primeiro treinamento em segurança cibernética, realizado por meio da plataforma *Proofpoint*. Este treinamento foi obrigatório para todos os servidores, estagiários e colaboradores do Rioprevidência que tinham algum tipo de acesso digital, como login, e-mail, entre outros.

Este treinamento teve duração de 120 minutos e abordou os seguintes temas:

- 1). Proteção de dados;
- 2). Ameaças internas;
- 3). E-mail e engenharia social (que incluía toda a parte de *phishing*).

O treinamento foi realizado antes dos testes de *phishing* com o objetivo de garantir que todos os usuários estivessem devidamente informados sobre as ameaças presentes no ambiente digital. Essa ação almejou aumentar a conscientização sobre os riscos e reforçar as práticas de segurança, preparando os usuários para reconhecer e enfrentar possíveis tentativas de fraude online.

Foram enviados vários alertas sobre o início do curso pela escola financeira e pela própria plataforma *proofpoint*.



SP Security Education Platform <awareness@securityeducation.com>
Para: [REDACTED]

Responder Responder a todos Encaminhar
Ter, 28/05/2024 13:45

Ola [REDACTED],

A equipe de TI do Rio Previdência está lançando uma nova iniciativa de treinamento em segurança. Estaremos compartilhando treinamento com fins educacionais que podem avaliar e melhorar sua inteligência de segurança cibernética no trabalho e em casa. Você tem um treinamento aguardando sua conclusão. Clique no link abaixo para iniciar seu treinamento, que deve ser entregue até May-31-2024.

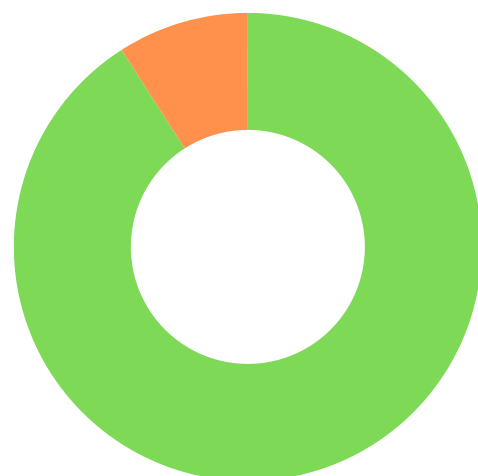
<https://rioprevidncia.ws01-securityeducation.com/ticketAuth/365d4daa39b94e978c95866539303d4f>

Se você tiver alguma dúvida ou comentário, entre em contato comigo pelo e-mail ppoint@rioprevidencia.rj.gov.br.

Obrigado,
Every Proofpoint

**Números da campanha
“treinamento de segurança
em TI: *phishing* e outros
perigos”.**

**Não completaram o treinamento
9.1%**



**Completaram o treinamento
90.9%**

No dia 25 de julho de 2024, ocorreu mais um treinamento no formato de workshop, em que foram discutidos temas como segurança digital e os riscos da internet.

A poster for a 'Workshop sobre Segurança Digital'. The title is in large white letters on a dark background. Below it, a yellow banner states the event is postponed to 25/07. The background features a network of dots and lines, a shield with a padlock, and hands holding a smartphone. The event details are listed with icons: date, time, location, and a list of bullet points with green checkmarks. At the bottom, there is a disclaimer and logos for Rioprevidência, Neotel, and Proderj.

WORKSHOP SOBRE SEGURANÇA DIGITAL

EVENTO ADIADO PARA 25/07
(os inscritos não precisam realizar uma nova inscrição)

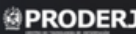
 25 de julho

 Às 14:00

 Av. Presidente Vargas, 1.100, Centro - DER, 14º andar

- ✓ PARA TODOS OS SERVIDORES DO RIOPREVIDÊNCIA
- ✓ PALESTRANTES:
SÂMYA MASSARI - VICE-PRESIDENTE DE GOVERNO DIGITAL PRODERJ
JOSÉ RICARDO MAIA - CTO | NEOTEL SEGURANÇA DIGITAL
- ✓ COM CERTIFICADO DE PARTICIPAÇÃO
- ✓ COFFEE BREAK

Excepcionalmente, devido à significativa demanda de Recenseamento Obrigatório, servidores, estagiários e terceirizados lotados nas agências, na COOAT e na COOPE devem permanecer normalmente em seus postos de trabalho.

👉 Um total de 151 pessoas, incluindo servidores, estagiários e terceirizados, participaram do evento.



1.2 Teste de *Phishing*

O objetivo de uma campanha de phishing é iludir os usuários para que realizem ações vantajosas para os cibercriminosos. **O sucesso da campanha é avaliado pela habilidade de enganar as vítimas e cumprir as metas dos criminosos.**

Para persuadir os usuários, foram empregadas técnicas psicológicas como autoridade, urgência e escassez, que aproveitam os instintos humanos. Essas estratégias, frequentemente utilizadas em ataques reais, aumentam a eficácia das simulações.

- **Autoridade:** Os atacantes se apresentam como figuras de autoridade para gerar confiança.
- **Urgência:** Eles criam um senso de urgência falso para estimular uma ação rápida, diminuindo a verificação.
- **Escassez:** Ofertas limitadas pressionam as vítimas a agir de forma impulsiva.

Campanhas de *phishing* são mais eficazes quando envolvem sites que imitam instituições governamentais, devido à confiança que a população deposita nesses órgãos.

Criminosos criam páginas falsas para simular serviços essenciais, como os da Receita Federal ou Previdência Social, e enviam e-mails fraudulentos pedindo a verificação de dados pessoais ou financeiros, resultando em muitas vítimas.

Estudos recentes confirmam essa tendência. Segundo o *Proofpoint* e o *Verizon Data Breach Report*, ataques de phishing relacionados a páginas governamentais estão entre os mais comuns em campanhas de engenharia social. Esses levantamentos indicam que até 40% dos incidentes de engenharia social envolvem o uso de credenciais roubadas para fins maliciosos (*Proofpoint*).

Tendo isso em mente, no dia **02 de setembro de 2024**, foram enviados **367** e-mails, distribuídos em três grupos de 94 e um grupo de 85, utilizando quatro modelos distintos: três relacionados a páginas governamentais e um de caráter privado. Cada modelo empregou uma das três técnicas de persuasão mencionadas anteriormente, conforme os temas a seguir:



SISPATRI

SISTEMA DE REGISTRO DE BENS
DOS AGENTES PÚBLICOS

Prezado Servidor

O senhor(a) (Nome do Servidor) não realizou a declaração de bens. Caso não seja regularizado até o dia 15/07/2024, as seguintes consequências serão aplicadas conforme a legislação vigente:

Sanções Administrativas: Advertência, suspensão e até demissão do cargo público, conforme Art. 13, 53º da Lei nº 8.429/1992.

Implicações Legais: Processos por improbidade administrativa, resultando em multas, ressarcimento ao erário, perda da função pública e suspensão dos direitos políticos, conforme os Artigos 9 e 11 da Lei nº 8.429/1992.

Para evitar tais consequências, solicitamos que acesse o Sispatri e regularize sua situação o mais breve possível.

[Acessar o Sispatri](#)

TEMA 1: SISPATRI

TEMA 2: SEI!RJ



Detectamos um acesso suspeito em sua conta no Sistema Eletrônico de Informações do Rio de Janeiro (SEIRJ).

Para garantir a segurança dos seus dados e evitar qualquer uso indevido, solicitamos que você revise imediatamente as atividades recentes da sua conta.

Data do Acesso Suspeito: 15/07/2024 às 10:30

Localização: Rio de Janeiro, Rio de Janeiro

Para verificar as atividades recentes e atualizar suas informações de segurança, clique no link abaixo e siga as instruções fornecidas:

[Atividades Recentes](#)



GOVERNO DO ESTADO
RIO DE JANEIRO



Olá, Servidor



Ter uma vida saudável é:

dormir
despreocupado,
sabendo que a
segurança da sua
saúde está garantida

O Bradesco Saúde está oferecendo condições especiais e descontos exclusivos em planos de saúde para servidores. Aproveite a cobertura, atendimento de qualidade e benefícios exclusivos para você e sua família

Quero aproveitar

Aproveite 50% de desconto em todos os planos de saúde da Bradesco durante 1 ano
Oferta limitada até o dia 15/07/2024

Bradesco Saúde

Para todas as idades

**50% de desconto
em todos os Planos**

apenas para servidores

- » Cobertura em todo território nacional
- » Reembolsos das despesas médico-hospitalares
- » Assistência ambulatorial e hospitalar com obstetrícia
- » Isenção de carências para terapias
- » Isenção de carências para cirurgia geral e internações clínicas.

TEMA 3: BRADESCO



Caro Servidor(a),

A Receita Federal faz anualmente uma análise detalhada da entrega do **Imposto de renda** e encontrou problemas relacionados ao CPF cadastrado para este e-mail, que devem ser regularizados com urgência.

Acesse o portal do E-CAC para regularizar os itens em pendência constatados no CPF cadastrado e evite problemas futuros.

A não regularização dos itens informados pode implicar na suspensão em recursos atrelados ao CPF cadastrado bem como multa previstos no Art 37 da Lei 10.522 de 19 de julho de 2002.

Acessar @cac

TEMA 4: RECEITA FEDERAL



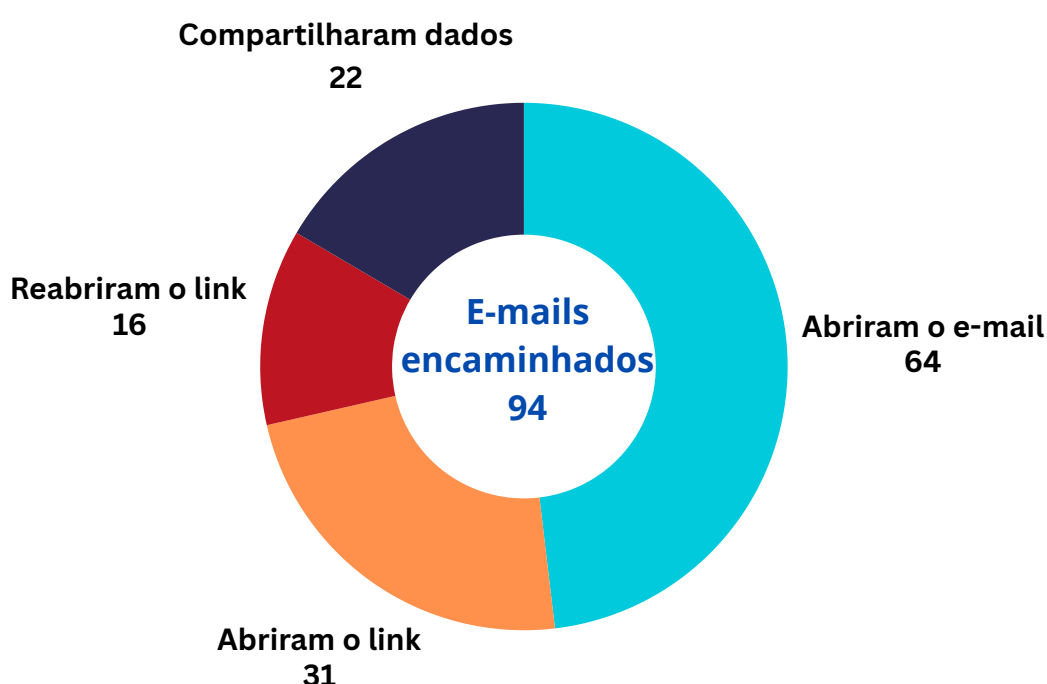
2 Resultados dos testes de phishing



2.1 GRUPO 1 - SISPATRI

A estratégia adotada neste grupo de e-mails foi a de **“urgência”**.

Essa técnica revelou-se extremamente eficaz para o grupo em questão, registrando a maior incidência de aberturas e reaberturas de links, além de um considerável índice de compartilhamento de informações.



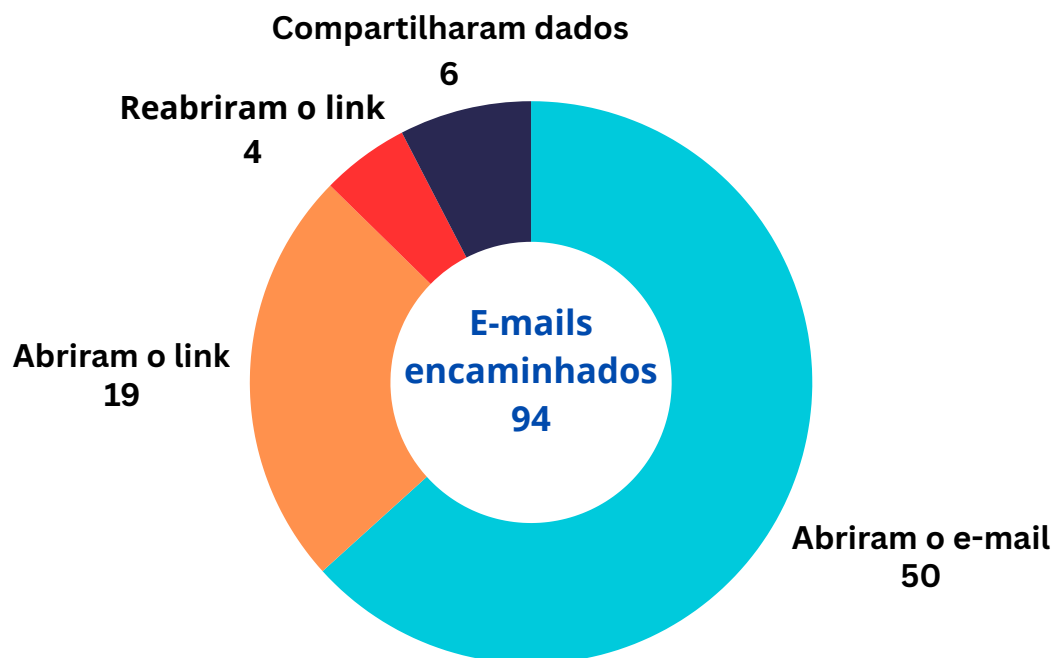
Dos 94 colaboradores que receberam os e-mails de *phishing*:

- 68% abriram o e-mail.
- 31% clicaram no link, dos quais 17% clicaram novamente;
- 23% submeteram dados.

2.2 GRUPO 2 - SEI!RJ

A estratégia adotada neste grupo de e-mails foi a de **“urgência”**.

Essa técnica mostrou-se eficaz para o grupo em questão, registrando a terceira maior taxa de abertura de links.



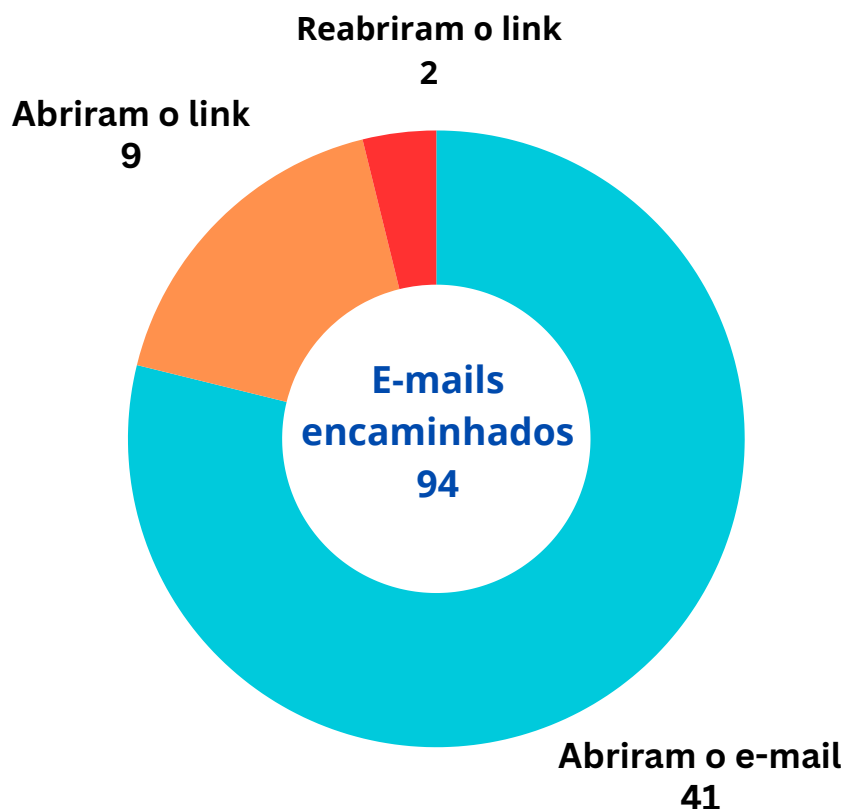
Dos 94 colaboradores que receberam os e-mails de *phishing*:

- 53% abriram o e-mail;
- 20% clicaram no link, dos quais 4% clicaram novamente;
- 6% submeteram dados.

2.3 GRUPO 3 - BRADESCO

A estratégia aplicada neste grupo de e-mails foi a de **"escassez"**.

Essa técnica, possivelmente devido ao fato de se tratar de uma empresa privada, resultou em poucos cliques, registrando a menor taxa de abertura de links e nenhuma submissão de dados.



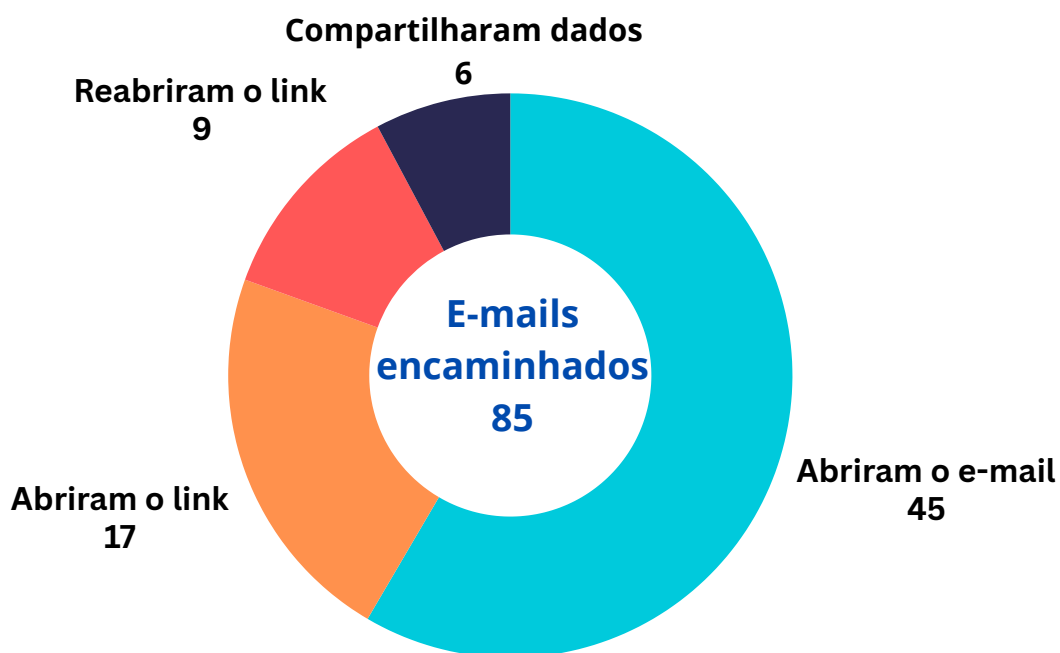
Dos 94 colaboradores que receberam os e-mails de *phishing*:

- 44% abriram o e-mail;
- 10% clicaram no link, dos quais 2% clicaram novamente;
- Ninguém submeteu dados.

2.4 GRUPO 4 - RECEITA FEDERAL

A estratégia adotada neste grupo de e-mails foi a de **“autoridade”**.

Essa técnica mostrou-se muito eficaz para o grupo em questão, sendo a segunda com maior índice de cliques e reaberturas de links, além de resultar em um número significativo de submissões de dados.



Dos 85 colaboradores que receberam os e-mails de *phishing*:

- 53% abriram o e-mail.
- 20% clicaram no link, dos quais 11% clicaram novamente ;
- 7% submeteram dados.

2.5 DISCUSSÃO DOS RESULTADOS

Os dados da campanha de phishing do RIOPREVIDÊNCIA mostram que, embora os resultados não tenham sido tão expressivos em termos percentuais, ainda há muito a ser feito em relação à conscientização. O ideal seria que não houvesse cliques nos *links* e, ainda mais importante, que não houvesse o compartilhamento de dados pessoais.

Apenas **8** usuários registraram formalmente os e-mails suspeitos, segundo a área de suporte em TI:

SOLID-012487 SOLID-012653
SOLID-012482 SOLID-012480
SOLID-012516 SOLID-012489
SOLID-012483 SOLID-012479

ATENÇÃO

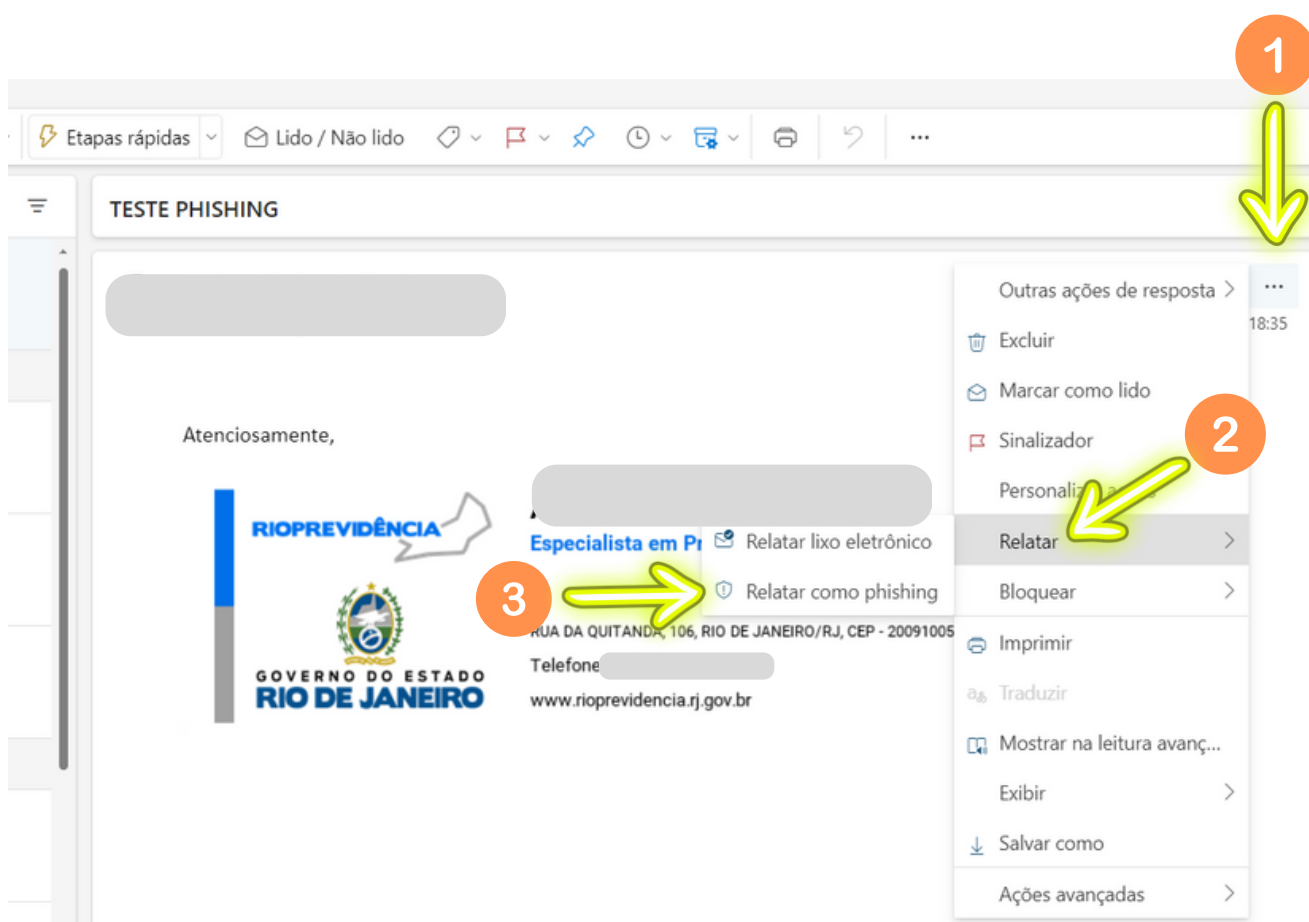


- Os ataques de *phishing* podem se manifestar de diversas maneiras e por meio de diferentes instituições, sejam elas públicas ou privadas.
- Um único clique em um *link* malicioso por parte de um usuário pode colocar em risco toda a segurança dos dados de uma organização.

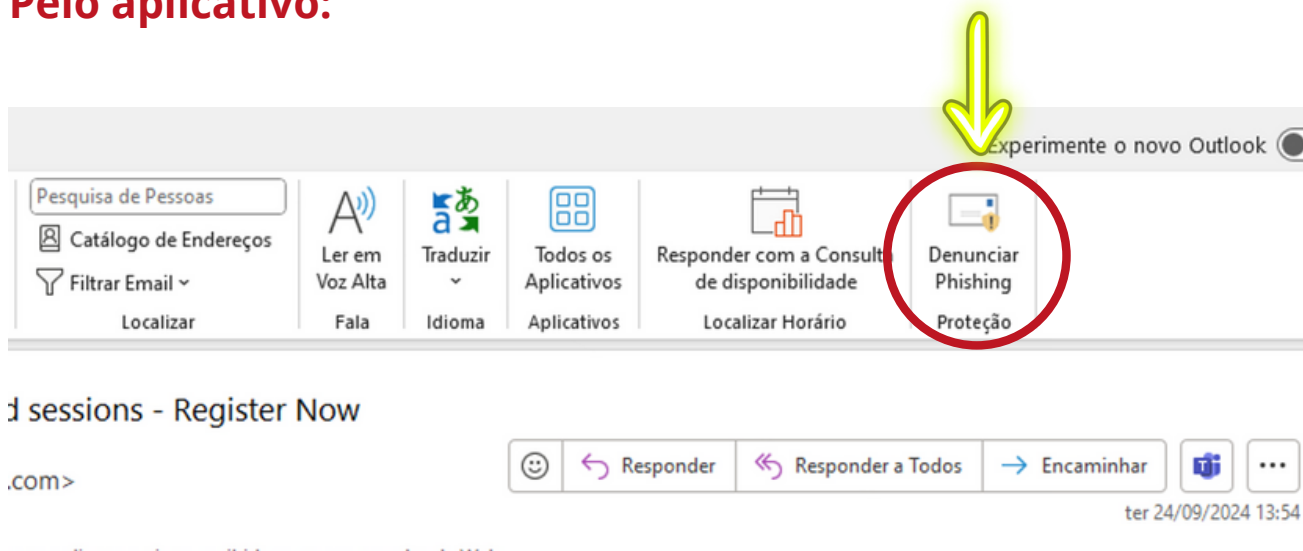
Ao identificar um e-mail suspeito, é fundamental que você registre essa suspeita imediatamente.

Existem maneiras de realizar esse registro diretamente no Outlook:

Pela web:



Pelo aplicativo:



Relatar tentativas de *phishing* é importante para prevenir fraudes e proteger informações, minimizando o risco de que essas ameaças se concretizem. Essa prática ajuda a identificar novas táticas criminosas, melhorando a detecção e resposta a ataques.

Denúncias rápidas podem evitar roubos de informação e dados e aumentar a conscientização sobre a gravidade desses ataques, promovendo uma cultura de segurança digital mais robusta.





Dicas importantes:



Identificação do Remetente

Sempre verifique o endereço de e-mail e desconfie de variações sutis.



Conteúdo do Mensagem

Mensagens que geram um sentimento de urgência ou apresentam ofertas extraordinárias costumam ser duvidosas.



Links e Anexos

Antes de clicar em um link, posicione o mouse sobre ele para conferir o endereço real de destino que aparece na barra inferior (na parte de baixo da tela).



Erros de Linguagem

Erros de gramática e ortografia são frequentemente sinais de *phishing*.



Dicas importantes:



Use Autenticação de Dois Fatores

Sempre que possível, ative essa funcionalidade para proteger suas contas.



Verifique a Fonte

Se a mensagem parece vir de uma empresa conhecida, acesse o site oficial diretamente em vez de clicar em links na mensagem.



Não Compartilhe Informações

Nunca forneça dados pessoais, senhas ou informações financeiras em resposta a e-mails.



Eduque-se e aos Outros

Compartilhe informações sobre *phishing* com amigos e familiares.

Referências

PROOFPOINT. Relatório sobre phishing: ameaças e tendências. [s.l.]: Proofpoint, 2023. Disponível em: https://www.proofpoint.com/br/resources/threat-reports/human-factor?utm_source=google&utm_medium=cpc&&utm_source=google&utm_medium=cpc&utm_term=proofpoint&placement=&gad_source=1&gclid=Cj0KCQjwr9m3BhDHARIsANut04ZyxO7HlmcqjAhEXF4E0onJr0pneuGANr-I9WT3_6IDYQTNJFBs9MoaAtxuEALw_wcB&gclsrc=aw.ds. Acesso em: 24 set. 2024.

VERIZON. Data Breach Investigations Report 2023. [s.l.]: Verizon, 2023. Disponível em: <https://www.verizon.com/business/resources/reports/dbir/>. Acesso em: 24 set. 2024.

EVERY. Relatório de simulação de *phishing* 1º ciclo. 2024