MAILSECURITY PROTECTION
The E-mails Security Experts

E-BOOK

2022

# Guia definitivo de estratégia de segurança cibernética de e-mail

## Uma abordagem centrada em pessoas para deter ransomware, ataques de malware, phishing e fraude de e-mail

mailsecurity.com.br

# E-mail: o seu vetor de ameaças mais crítico

## Todos os dias, no mundo todo, uma batalha silenciosa se dá em um dos recursos mais familiares e indispensáveis do trabalho moderno: a caixa de entrada de e-mail.

Como principal vetor de entrega de malware e terreno fértil para todos os tipos de fraude, o e-mail é o canal no qual os atacantes cibernéticos têm mais possibilidades de comprometer seus alvos. Eles induzem os usuários a clicar em links inseguros, a fornecer suas credenciais ou até mesmo a executar comandos diretamente (por exemplo, para enviar dinheiro ou arquivos confidenciais).

Não é difícil entender porque os atacantes preferem o e-mail. Ele usa uma arquitetura de décadas atrás que não foi desenvolvida levando em consideração a segurança. Ele é universal. E, diferentemente do hardware e da infraestrutura de computadores, os ataques de e-mail exploram vulnerabilidades que não podem ser corrigidas: pessoas.

O desafio se torna ainda mais complicado em meio a uma migração para nuvem e trabalho remoto.

As organizações gastam bilhões por ano em ferramentas de segurança desenvolvidas para reforçar o perímetro de rede, detectar intrusões de rede e proteger endpoints. Mesmo assim, o volume — e os custos — do ransomware, do comprometimento de e-mail corporativo (BEC), do phishing de credenciais e das violações de dados causadas por malware nunca foram tão altos.[1]

Isso acontece porque os ataques de hoje "hackeiam" a natureza humana, e não apenas a tecnologia. E o e-mail é a maneira mais fácil de contactar pessoas.

## Considere estas descobertas de pesquisa:

**US$ 14,8 milhões**

são os custos médios anuais do phishing para uma organização grande — mais que o triplo da média de 2015[2]

**86%**

das organizações enfrentaram ataques de bulk phishing em 2021[3]

**77%**

das organizações enfrentaram ataques de comprometimento de e-mail corporativo (BEC) em 2021[4]

**78%**

das organizações viram ataques de ransomware baseados em e-mail em 2021[5]

**85%**

das violações de dados envolvem pessoas[6]

1 Ponemon Institute. "The 2021 Cost of Phishing Study" (Estudo sobre o custo do phishing em 2021). Junho de 2021.
2 Ponemon Institute. "The 2021 Cost of Phishing Study" (Estudo sobre o custo do phishing em 2021). Junho de 2021.
3 Proofpoint. "2022 State of the Phish". Fevereiro de 2022.
4 Ibid.
5 Ibid.
6 Verizon. "Data Breach Investigations Report Executive Summary" (Resumo executivo do relatório de investigações de violações de dados). Maio de 2021.

É hora de uma nova abordagem. O cenário de ameaças de hoje em dia pede uma mentalidade aberta e uma nova estratégia — uma cujo foco esteja na proteção de pessoas em vez da infraestrutura.

Não importa se você lidera o centro de operações de segurança de uma multinacional ou uma equipe de segurança minúscula; considere este guia como um ponto de partida. Vamos explorar:

- Por que o e-mail deve ser a sua prioridade de segurança nº 1
- O que o torna tão difícil de proteger
- Como uma segurança integrada, em camadas e centrada em pessoas é mais eficaz
- Onde otimizar as suas operações de segurança de e-mail para economizar dinheiro e simplificar a resposta

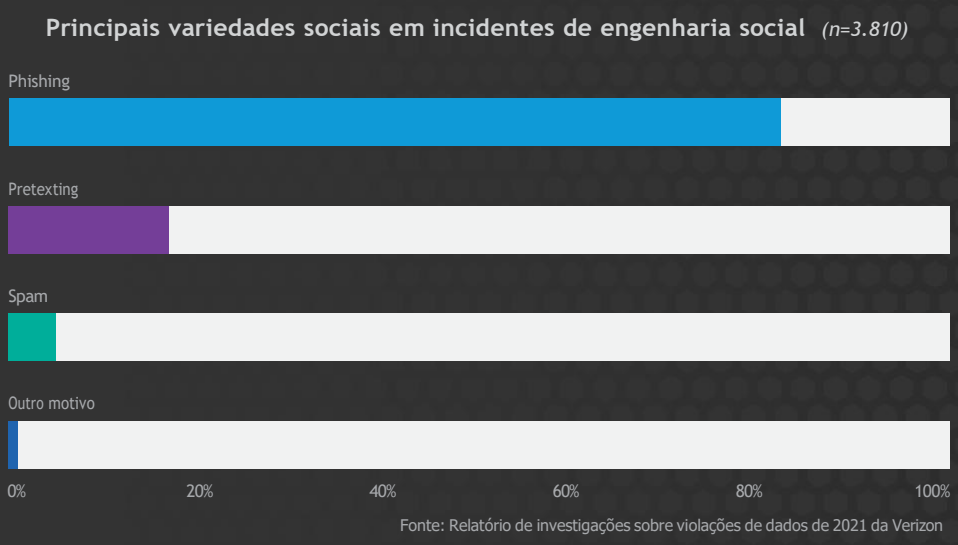



**Figura 1. Principais formas de engenharia social**

SEÇÃO 1

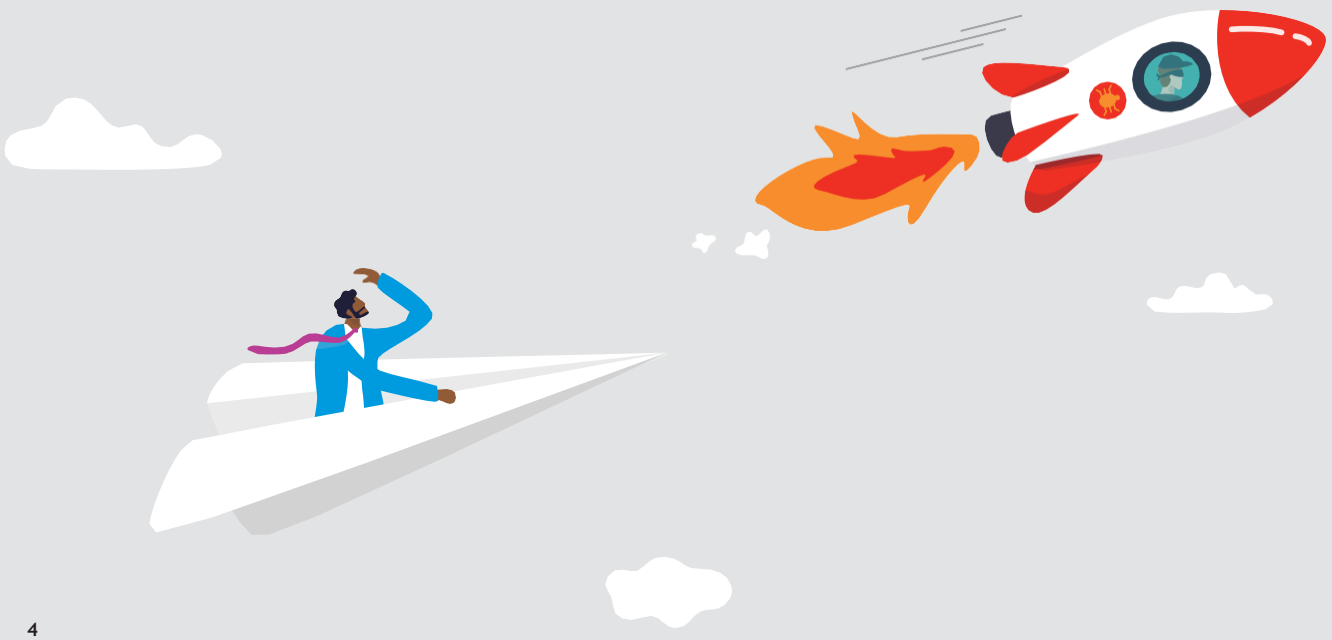
# Os ataques cibernéticos estão evoluindo mais rapidamente que as defesas tradicionais

## Proteger o e-mail é fundamental para a proteção da empresa. Porém, é um desafio complexo.

Isso porque as ameaças de e-mail são numerosas e amplamente diversificadas. As técnicas de ataque estão evoluindo constantemente. E a natureza humana — o elo mais fraco de toda organização — é um alvo perpétuo.

Não surpreende que soluções criadas para combater os ataques de apenas dois ou três anos atrás tenham dificuldades para acompanhar os novos tempos.

Esta seção descreve apenas algumas das maneiras pelas quais os atacantes cibernéticos visam pessoas. (Em muitos casos, os atacantes combinam técnicas para evitar as defesas e incrementar suas taxas de sucesso).



# Ransomware

O ransomware é uma ameaça antiga que persiste como um problema dos dias atuais. Esse tipo de malware — cujo nome deriva do pagamento ("ransom", em inglês) exigido após ele bloquear os arquivos das vítimas – é um grande problema para as empresas modernas. Trata-se de uma das formas mais perturbadoras de ataque cibernético de hoje em dia.

Grandes incidentes envolvendo infraestruturas de combustíveis,[7] alimentos[8] e saúde[9] em 2021 demonstraram que nenhum alvo está fora de cogitação.

Aproximadamente três quartos do ransomware começa, direta ou indiretamente, com um e-mail de phishing.[10] Esses e-mails induzem os usuários a abrir um anexo malicioso ou a clicar em um URL malicioso.

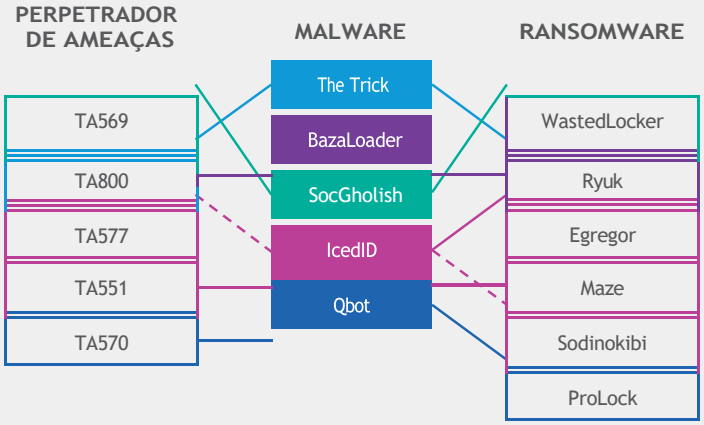



**Figura 2. Ligações entre perpetradores de ameaças, malware de primeiro estágio e ransomware**

A maior parte do ransomware é entregue como uma infecção secundária, depois que o sistema já foi infectado por um cavalo de Troia ou carregador. Em seguida, muitos atacantes especializados nesses cavalos de Troia ou carregadores vendem o acesso a organizações de ransomware. Para a maioria das organizações, a primeira linha de defesa contra o ransomware consiste em assegurar que elas estejam protegidas contra outros tipos de malware.

Não há um relacionamento simples e direto entre o malware de acesso inicial e a cepa de ransomware distribuída para as vítimas. Porém, pesquisadores da Proofpoint e de outras empresas do setor observaram algumas associações proeminentes, conforme mostrado na figura 2.

7 David E. Sanger, Clifford Krauss, Nicole Perlroth (New York Times) "Cyberattack Forces a Shutdown of a Top U.S. Pipeline" (Ataque cibernético causa desligamento de um importante oleoduto nos EUA). Maio de 2021.
8 Julie Creswell, Nicole Perlroth, Noam Schreiber (New York Times) "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business" (Ransomware interrompe operações de processamento de carnes em empresa crítica para os EUA). Junho de 2021.
9 Nicole Perlroth, Adam Satariano (New York Times) "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks" (Hospitais irlandeses são os mais recentemente atingidos por ataques de ransomware). Maio de 2021.
10 Unit 42, Palo Alto Networks. "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report" (Famílias de ransomware: dados de 2021 para complementar o Relatório de ameaças de ransomware da Unit 42). Julho de 2021.

# Fraude de e-mail e comprometimento de e-mail corporativo (BEC)

O comprometimento de e-mail corporativo (BEC), também conhecido como fraude de e-mail, é uma das ameaças mais onerosas e menos compreendidas da segurança cibernética. Essa categoria de fraude de e-mail de rápido crescimento nem sempre chama tanta atenção quanto outros crimes cibernéticos de alto padrão. Porém, em termos de custos financeiros diretos, o BEC supera facilmente outros tipos de ameaça.

Só em 2020, esquemas de BEC custaram mais de US$ 1,8 bilhão a organizações e indivíduos.[11] Isso é mais de US$ 100 milhões acima do valor registrado em 2019 e 44% do total de perdas por crime cibernético.

Os ataques de BEC são difíceis de detectar. Eles não têm as cargas habituais — arquivos anexados ou URLs maliciosos — que podemos analisar. Em vez disso, os fraudadores recorrem à impostura e a outras técnicas de engenharia social para enganar as pessoas.

Muitos dos esquemas de BEC de hoje em dia são altamente sofisticados, bem financiados e respaldados por pesquisa e planejamento cuidadosos. Um número crescente de atacantes está concentrando seus esforços na fraude de fatura de fornecedor e no sequestro de grandes transações entre empresas (B2B).

Os ataques de BEC aproveitam-se da natureza humana. Eles exploram a confiança das pessoas.

**Veja como eles atuam:**

1. Primeiro, os atacantes de BEC passam-se por uma pessoa ou entidade na qual o destinatário pode confiar, como um colega, chefe ou fornecedor.
2. O atacante envia um e-mail instruindo os destinatários a realizar uma ação que desvia dinheiro ou informações financeiras confidenciais da organização. Isso pode incluir transferências bancárias fraudulentas, faturas falsas, folhas de pagamento desviadas, dados bancários alterados para pagamentos futuros e inúmeros outros esquemas.
3. Frequentemente, quando a organização descobre o erro, já é tarde demais para recuperar o dinheiro.

### TIPOS DE BEC

O comprometimento de e-mail corporativo (BEC) pode se apresentar de várias formas — limitadas apenas pela criatividade dos atacantes. Seguem seis tipos comuns:

1. **Fraude de fatura.** Esse ataque induz as vítimas a pagar faturas falsas ou a desviar pagamentos legítimos.
2. **Redirecionamento de folha de pagamento.** Nesse esquema, atacantes fazendo-se passar por funcionários pedem ao departamento pessoal que pague os salários em sua conta.
3. **Extorsão.** Neste caso, os atacantes ameaçam causar danos ou constrangimentos caso a vítima não pague o resgate.
4. **Iscas e tarefas.** Estas enganam as vítimas com uma pergunta simples, como "Você está aí?", e daí passam para outras formas de BEC.
5. **Fraude de cartão de presente.** Esta técnica induz os destinatários a comprar cartões de presente e enviar o número e o PIN de cada cartão para o fraudador.
6. **Fraude de pagamento adiantado.** Nesse golpe antigo, vigaristas pedem dinheiro para desbloquear uma soma ainda maior — que a vítima nunca recebe.

11 FBI. "Internet Crime Report 2020" (Relatório de crimes de Internet de 2020). Março de 2021.

# Sequestro/comprometimento de contas

O comprometimento de uma conta é o ato de obter, maliciosamente, controle sobre uma conta de e-mail ou de um serviço de nuvem de um usuário legítimo — o que dá ao atacante amplo acesso a dados, contatos, itens de agenda e e-mail.

Além dos dados do usuário comprometido, o atacante pode utilizar a conta para se fazer passar pelo usuário em ataques de engenharia social, tanto dentro quanto fora da organização. Isso inclui comprometimento de e-mail corporativo (BEC), ataques a cadeias de fornecimento e mais.

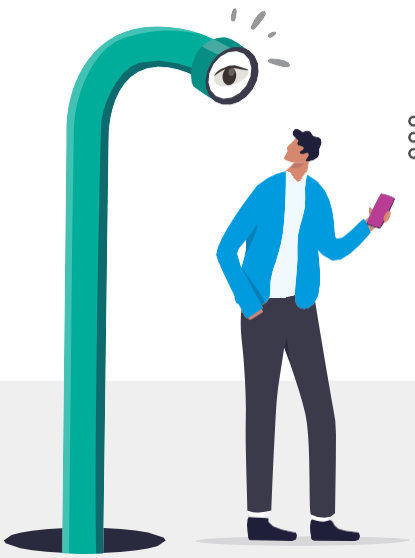
Os perpetradores de ameaças podem acessar dados confidenciais, persuadir usuários ou parceiros comerciais externos a transferir dinheiro ou causar danos à reputação e às finanças de uma organização. Ou, pior ainda, podem instalar "backdoors" para preservar o acesso para ataques futuros.

## Anatomia de um sequestro de conta

Veja como a maioria dos sequestros de contas ocorre.

**Roubo de credenciais.** O atacante obtém acesso às credenciais do usuário por meio de phishing de credenciais (que, sozinho, representa aproximadamente dois terços de todo o volume de phishing), ataques de força bruta contra senhas, reutilização/reciclagem de credenciais ou malware de roubo de credenciais.

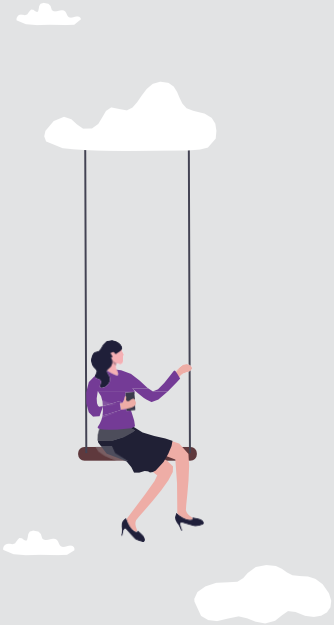
**Infiltração.** Após efetuar login na conta do usuário, o atacante tem acesso ao e-mail, aos contatos, à agenda e aos arquivos da vítima. O atacante pode roubar esses dados diretamente ou utilizá-los para se fazer passar pelo usuário de forma convincente. Alguns fraudadores podem responder a threads de e-mail existentes ou enviar rascunhos de e-mail com malware ou URLs inseguros para colegas e parceiros comerciais externos. Apresentando-se como os verdadeiros usuários, eles podem visar outras pessoas dentro e fora da empresa com faturas falsas ou instruções para redirecionamento de pagamentos. O atacante também pode fazer upload de malware em compartilhamentos de arquivos corporativos ou sabotar a empresa de outras maneiras.



**Persistência.** Frequentemente, o atacante cria sub-repticiamente regras de encaminhamento automático que dão acesso ao e-mail do usuário mesmo que este altere a senha. A possibilidade de ver todos os e-mails recebidos e convites da agenda dá ao atacante informações para futuros ataques de impostura.

SEÇÃO 2

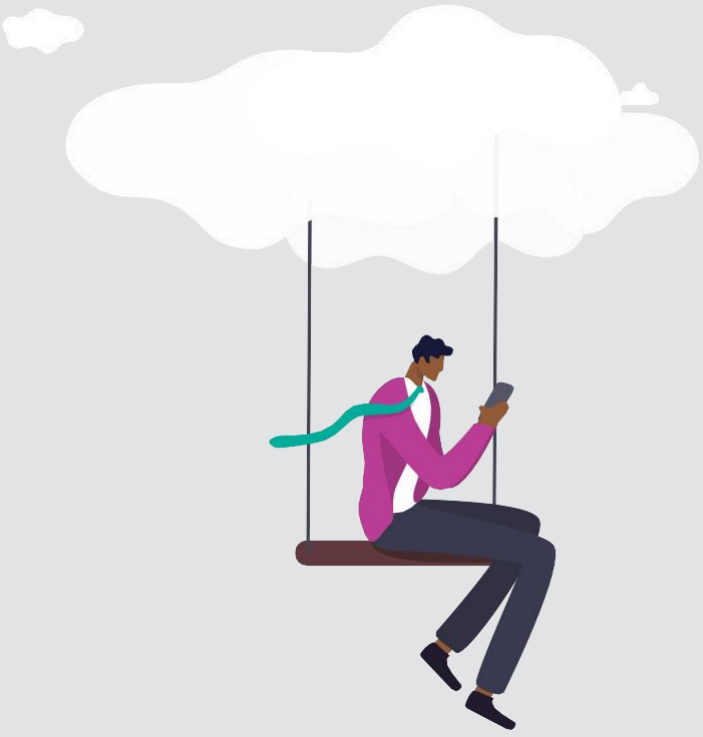
# Como o cenário de ameaças mudou

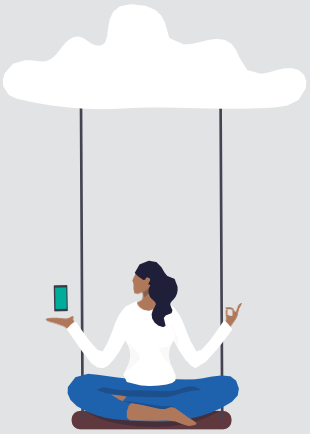


## A força de trabalho remota e híbrida de hoje em dia é viabilizada pelas tecnologias de nuvem e móveis.

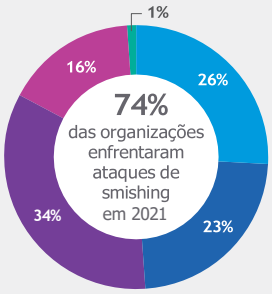
Os perímetros reforçados e as estruturas de rede tradicionais do passado já não existem mais. As pessoas são o novo perímetro.

Infelizmente, a maioria dos orçamentos de segurança — presos a outras prioridades e categorias de produtos — não acompanhou essa realidade.



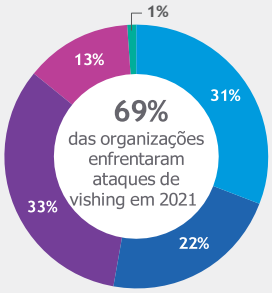


Volume de ataques de smishing

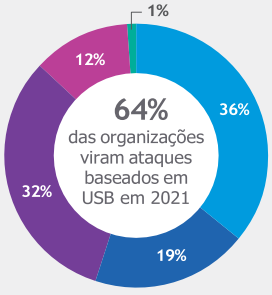


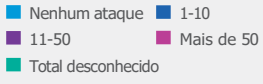

Volume de ataques em mídias sociais


Volume de vishing




Volume de pen drives "esquecidos" propositalmente




Fonte: State of the Phish, 2022

# Os atacantes visam pessoas e não infraestruturas

Mesmo gastando bilhões por ano para incrementar sua infraestrutura, as organizações podem estar negligenciando os riscos de segurança mais importantes, baseados em pessoas. As pessoas são o ponto de entrada mais fácil e mais lucrativo no seu ambiente.

Segundo o "Relatório de investigações de violações de dados da Verizon", impressionantes 85% das violações de dados envolvem pessoas.[12] Os seus usuários estão sob um bombardeio constante de hiperlinks inseguros, anexos maliciosos, roubo de credenciais, esquemas de engenharia social e ameaças de impostores.

# Os ataques frequentemente se estendem por múltiplos vetores

Visar pessoas significa interagir com elas nas ferramentas e plataformas que elas utilizam. Aonde os usuários vão, os atacantes os seguem.

Os fluxos de trabalho modernos são dinâmicos e imprevisíveis. O usuário pode iniciar uma conversa por e-mail, agendar uma reunião subsequente em um aplicativo de chat e colaborar em arquivos armazenados na nuvem.

Os ataques modernos também são dinâmicos e imprevisíveis. Eles se desenvolvem em múltiplos canais, utilizam uma variedade de táticas e ferramentas e pegam carona em todas as plataformas que as pessoas utilizam para trabalhar.

Um ataque pode começar com um e-mail e um link para malware hospedado em um site de compartilhamento de arquivos. Ou um aplicativo de nuvem clandestino pode roubar credenciais para comprometer uma conta legítima e utilizá-la para lançar ataques de BEC.

O desafio não para de crescer. Frequentemente, um perpetrador de ameaças avançado cria o "produto" malware e configura a infraestrutura como um pacote ou serviço fácil de usar. Criminosos cibernéticos de baixo nível podem alugar o serviço para seus ataques, pagando para utilizá-lo por um determinado período de tempo ou oferecendo uma parte dos ganhos em cada comprometimento bem-sucedido. Em outros casos, eles atuam como distribuidores, enviando e-mails com o malware e ganhando uma comissão sobre cada infecção bem-sucedida.

12 Verizon. "Data Breach Investigations Report Executive Summary" (Resumo executivo do relatório de investigações de violações de dados). Maio de 2021.

# Não basta defender cada setor

As organizações podem compreender a natureza multifacetada e centrada em pessoas das ameaças atuais e investir em ferramentas de segurança para cobrir cada risco em potencial. No entanto, se essas ferramentas não trabalharem juntas de forma coordenada, elas não poderão oferecer a visibilidade e os insights de que as equipes de segurança precisam para gerenciar o risco.

Imagine um time de craques de futebol que não treinam juntos, uma orquestra de virtuosos que nunca ouvem os demais instrumentos ou uma equipe cirúrgica que não chega a um consenso sobre como tratar um paciente. Não importa o quão habilidoso é cada indivíduo, ele não pode ser tão eficaz quanto uma equipe bem coordenada.

Os atacantes de hoje combinam técnicas para ataques mais sofisticados. Ferramentas de produtos individuais criam complexidades desnecessárias para equipes de segurança que já estão com dificuldades para gerenciar apenas o risco atual. É por isso que uma segurança realmente centrada em pessoas requer uma abordagem holística e coordenada.

SEÇÃO 3

# Foco nos seus usuários mais arriscados

O primeiro passo para proteger os usuários é identificar quais constituem um risco maior. Embora cada organização possa ponderar os vários fatores de risco diferentemente, todas devem considerar alguma combinação de vulnerabilidade, ataques e privilégio.

Vulnerabilidade é uma forma de determinar quem está mais propenso a ser vítima de uma ameaça. Uma análise do ataque pode revelar quem está sendo visado na sua organização, com que intensidade e por quais tipos de ameaças. O privilégio, por sua vez, pode ajudar a prever o quão danoso um ataque bem-sucedido seria para a organização.

Concentre-se nos usuários que constituem um risco acima do normal, com base em qualquer combinação desses fatores. A situação desses usuários requer atenção extra por parte da equipe de segurança e das partes interessadas, as quais devem saber como e porque eles estão em risco.

Esse nível de visibilidade em todas as três áreas é essencial para uma segurança centrada em pessoas. Sem isso, as organizações não têm meios de saber quem precisa de camadas adicionais de segurança ou como proteger melhor os usuários.


# Vulnerabilidade: como as pessoas trabalham e no que elas clicam

Quantificar a vulnerabilidade não é fácil com ferramentas de segurança baseadas em tecnologias tradicionais. Porém, com uma abordagem centrada em pessoas, você pode mensurar como elas trabalham e no que elas clicam.

"Como elas trabalham" abrange as ferramentas, sistemas e plataformas que elas utilizam em seu trabalho. "No que elas clicam" é uma medida do seu nível de conscientização quanto à segurança e de sua propensão a se deixar enganar por táticas de ameaças prováveis.

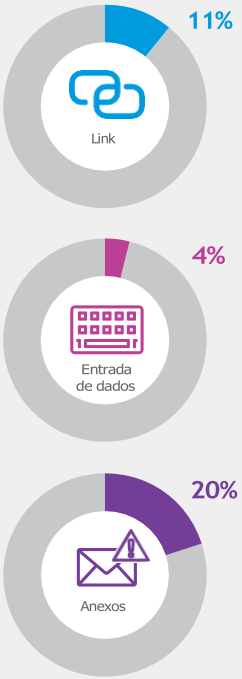
## Como o seu pessoal trabalha

Você pode ter uma ideia geral da vulnerabilidade dos usuários determinando quais ferramentas, plataformas e aplicativos eles usam. Isso pode incluir:

- Quais aplicativos de nuvem eles utilizam e se esses aplicativos são aprovados pelo departamento de TI
- Quantos e quais dispositivos eles utilizam para acessar e-mail
- Se tais dispositivos são seguros
- Se os usuários exercitam uma boa higiene digital, como usar senhas fortes e não repetidas e manter o software atualizado
- Se eles utilizam consistentemente autenticação por múltiplos fatores para acesso corporativo e até mesmo em contas pessoais

Quanto mais granular for a sua visibilidade, melhor.

**Tipos de modelo de phishing: taxas de falha médias**




Fonte: State of the Phish, 2022

## No que o seu pessoal clica

A vulnerabilidade pode ser medida mais precisamente com base em educação sobre segurança, simulações de phishing e como os usuários respondem a ameaças reais.

O treinamento para conscientização quanto à segurança, camada essencial de uma estratégia de segurança eficaz, pode oferecer insights sobre quais usuários são os menos preparados para reconhecer, resistir e denunciar ameaças cibernéticas. Em geral, os usuários que se saem mal em exercícios de treinamento — ou que não fazem tais exercícios — são mais vulneráveis que os usuários bem avaliados.

Fora deixar que os atacantes entrem e ver quem clica em um link, preenche um formulário ou abre um arquivo, as simulações de phishing são uma das maneiras mais poderosas de se avaliar esse aspecto de vulnerabilidade.

Finalmente e o mais importante, rastrear os usuários que se relacionam com e-mails sabidamente maliciosos, mesmo quando o clique é bloqueado, isolado ou reescrito.

Tais dados do mundo real, combinados com informações de conscientização quanto à segurança, dão a você uma visão holística sobre a vulnerabilidade do e-mail ao rastrear a conclusão dos treinamentos, simulações de phishing e interações com mensagens maliciosas reais.

## Ataques: como as pessoas são visadas

Todo ataque cibernético é potencialmente danoso. Contudo, alguns são mais perigosos, direcionados ou sofisticados que outros. É por isso que medir esse aspecto do risco pode ser mais complicado do que parece.

Ameaças "comoditizadas" e indiscriminadas podem ser mais numerosas que outros tipos de ameaças. Mas elas são bem compreendidas e mais facilmente bloqueadas.

Outras ameaças podem aparecer em apenas uns poucos ataques. Mas elas podem representar um perigo mais grave devido à sua sofisticação ou às pessoas visadas.

Saber a diferença é fundamental para identificar os usuários que estão sob um risco maior. Na Proofpoint, chamamos esses usuários de "Very Attacked People™" (VAP ou "pessoas muito atacadas"). Ter uma visão completa de todo o tráfego de e-mail e correlacioná-la a uma inteligência detalhada contra ameaças é fundamental para quantificar quem está sendo visado e com que intensidade.

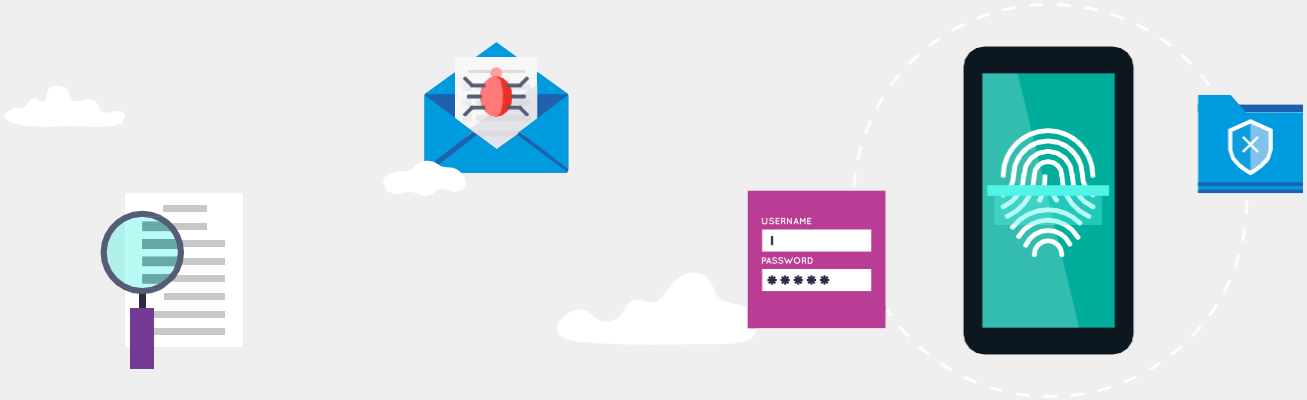
**Os fatores que devem pesar mais na avaliação de cada usuário incluem:**

- A sofisticação do criminoso cibernético
- O alcance e o foco dos ataques
- O tipo de ataque
- Volume total do ataque

Você também deve ponderar esses fatores no contexto dos departamentos, grupos ou divisões aos quais o usuário individual pertence.

Por exemplo, alguns usuários podem não estar em risco com base no volume ou no tipo de e-mail malicioso enviado a eles diretamente. Mas eles podem constituir um risco maior por trabalharem em um departamento altamente atacado — e, portanto, estarem mais sujeitos a serem um alvo-chave no futuro.

Uma boa inteligência contra ameaças pode determinar quais ferramentas os atacantes estão utilizando e vincular incidentes aparentemente distintos a campanhas maiores.



# Privilégio: ao que as pessoas têm acesso

A medição do privilégio do usuário começa com a realização de um inventário de todas as coisas potencialmente valiosas às quais as pessoas têm acesso: dados, autoridade financeira, relacionamentos importantes e mais. Você deve saber onde se encontram os seus dados mais confidenciais e quem ou quais aplicativos têm acesso a eles.

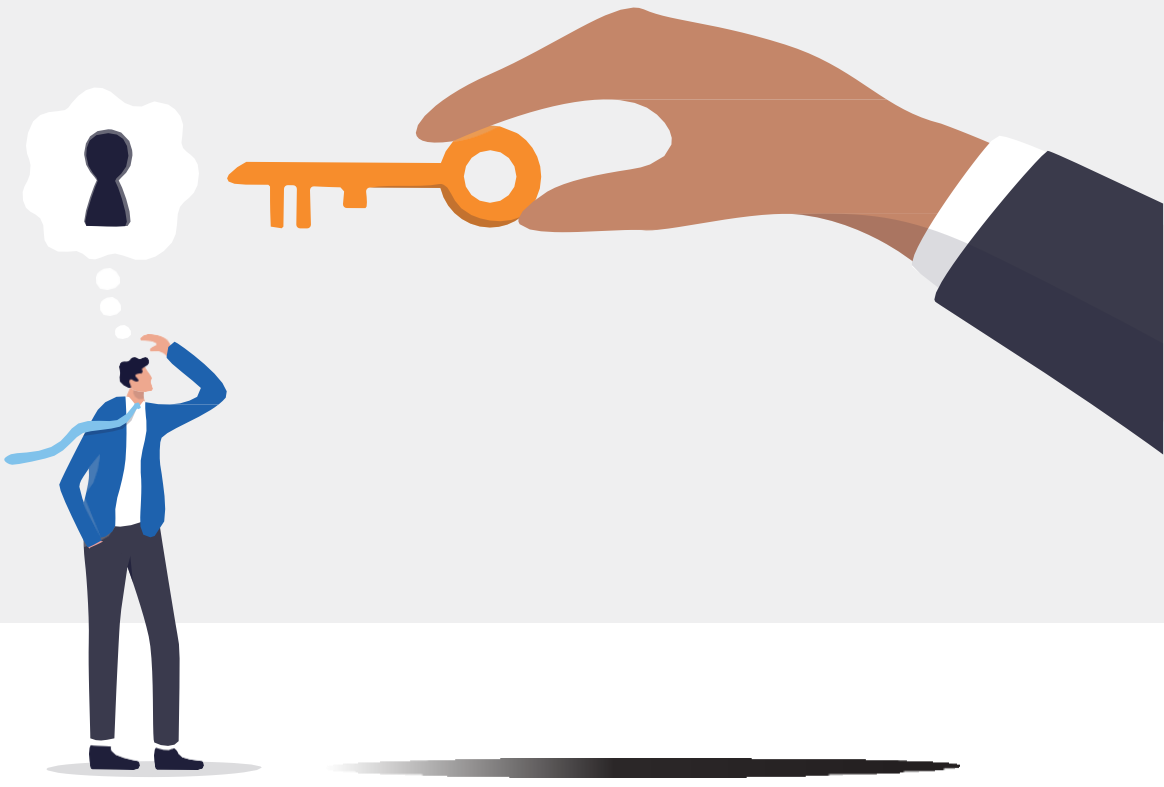
Usuários com acesso a sistemas críticos ou a propriedade intelectual, por exemplo, podem precisar de proteção extra, mesmo quando não estão particularmente vulneráveis ou no radar dos atacantes.

A posição do usuário no gráfico organizacional é, naturalmente, um fator que influencia a pontuação do privilégio. Mas não é o único fator — e muitas vezes nem é o mais importante.

Um assistente administrativo pode ser um alvo mais atraente do que um gerente de nível intermediário para espionagem corporativa se o assistente tiver acesso à agenda do CEO. Da mesma forma, uma enfermeira com acesso a registros de pacientes de um hospital pode ser um alvo mais útil do que o CEO para ladrões de identidades.

Para os atacantes, um alvo valioso pode ser qualquer um capaz de atuar como um meio para um fim.

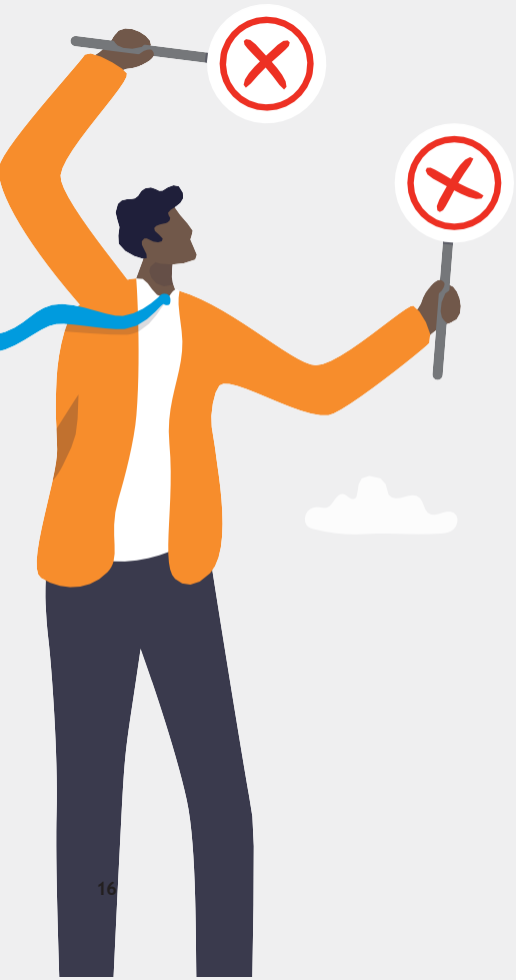
Proteger usuários de alto privilégio contra ataques externos é fundamental. Igualmente importante é proteger a sua organização contra usuários de alto privilégio. Nas mãos erradas, o acesso interno pode ser mal utilizado por malícia, negligência ou comprometimento. Contas comprometidas podem exportar arquivos confidenciais ou tentar comprometer ou fraudar outros usuários internos.



SEÇÃO 4

# Construção de uma defesa centrada em pessoas

Uma abordagem centrada em pessoas mantém todos protegidos aplicando controles correspondentes ao nível de risco de cada um. Isso funciona de forma unificada em todas as plataformas que as pessoas utilizam, contra todas as táticas que os atacantes empregam e em todos os vetores de ameaças que importam.



# Camada base: segurança para todos

Como os ataques por e-mail assumem diversas formas, você precisa de uma defesa que detenha toda a variedade de ameaças de e-mail, e não apenas algumas delas.

**Seguem as etapas mais essenciais para uma defesa de e-mail construída para ameaças modernas:**

- Detenha anexos e URLs maliciosos antes que estes cheguem às caixas de entrada dos usuários.
- Detenha ameaças de impostura sem cargas virais, como BEC e outras fraudes, incluindo as que se originam de contas de e-mail comprometidas dentro da sua própria organização ou de fornecedores.
- Proteja a navegação na Web e o e-mail pessoal dos usuários com o isolamento de e-mail pessoal e da Web.
- Torne os usuários mais resilientes com treinamento para conscientização quanto à segurança e dicas contextuais.
- Aplique controles, como o isolamento da Web, para afastar do seu ambiente os hábitos de navegação potencialmente inseguros dos usuários.
- Considere a proteção dos dados na sua estratégia de segurança de e-mail.

## Detenha anexos e URLs maliciosos antes que estes cheguem às caixas de entrada dos usuários

A maioria dos ataques cibernéticos dependem de que a vítima em questão faça alguma coisa — em muitos casos, que abra um anexo ou que clique em um URL. Porém, esses ataques ativados por seres humanos não podem ter êxito se a vítima em questão não chegar a ver a mensagem.

É aí que entra a proteção de segurança de e-mail avançada. Ao deter cargas maliciosas antes que estas cheguem às caixas de entrada dos usuários, uma solução eficaz pode proteger contra uma ampla variedade de ameaças de malware, inclusive ransomware, cavalos de Troia bancários, cavalos de Troia de acesso remoto, ladrões de informações, downloaders, redes de bots e mais.

## Detenha ameaças de impostura difíceis de detectar

Deter o malware é importante, mas alguns dos ataques de e-mail mais danosos não usam carga viral alguma. Em vez disso, eles contam com engenharia social.

O comprometimento de e-mail corporativo (BEC) é um exemplo. Ataques de BEC foram relatados em todos os 50 estados dos EUA e em 177 países, com transferências fraudulentas enviadas para pelo menos 140 países, segundo o FBI.[13]

No BEC e em outras formas de fraude de e-mail, o golpista faz-se passar por uma pessoa da confiança do destinatário utilizando uma conta de e-mail falsificada, comprometida ou parecida. Sob essa falsa identidade, o atacante pede à vítima que faça algo em benefício do atacante — como enviar dinheiro para uma conta bancária no exterior, enviar arquivos confidenciais etc.

As ameaças de impostura são um problema complexo e com muitas facetas. Para detê-las, você precisa de uma defesa em camadas que proteja os e-mails recebidos, enviados e internos — e que funcione de uma maneira holística e coesa.

13 FBI. "Internet Crime Report 2020" (Relatório de crimes de Internet de 2020). Março de 2021.

Juntamente com a educação do usuário e outros controles de segurança descritos nesta seção, seguem os principais elementos de uma defesa contra e-mails impostores.

## DMARC

Autenticação de e-mail por DMARC (Deploy Domain-based Message Authentication, Reporting and Conformance). DMARC é uma política em nível de Internet que comprova que o remetente do e-mail é quem ele afirma ser e que está autorizado a enviar em nome da organização.

Com DMARC, você obtém visibilidade sobre todos os e-mails enviados utilizando o seu domínio de e-mail, inclusive remetentes de terceiros confiáveis, como Marketo, Salesforce e outros. Com essa visibilidade, você pode autorizar todos os remetentes válidos que tentarem enviar e-mail em seu nome — e bloquear qualquer um que use os seus domínios confiáveis para roubar dinheiro ou prejudicar a sua marca.

## Classificação dinâmica

Embora o DMARC possa ajudar a deter ameaças que falsificam o seu domínio, os atacantes utilizam outras técnicas para enganar os usuários. É por isso que um outro componente fundamental para deter ameaças sem malware é analisar e classificar dinamicamente o conteúdo dos e-mails. Esse aspecto da segurança de e-mail consiste em analisar o que está no e-mail, e não apenas de onde ele vem. Por isso você precisa de uma segurança de e-mail que possa examinar indícios de fraude e bloquear ou estudar mais detalhadamente qualquer coisa que pareça insegura. A classificação dinâmica analisa e gerencia o e-mail com base em diversos fatores, inclusive:

- A reputação do remetente, o endereço IP e o cabeçalho do e-mail
- Análise do conteúdo baseada em autoaprendizagem para procurar frases, palavras e alterações do endereço de resposta
- O relacionamento entre o remetente e o destinatário
- Contexto sobre o remetente, por exemplo, se ele parece estar se fazendo passar por um fornecedor conhecido

## Insights sobre risco de fornecedor e defesa de e-mail interno

Em alguns casos, os atacantes nem tentam disfarçar seu endereço de e-mail — eles simplesmente assumem o controle sobre uma conta legítima da organização ou de um parceiro ou fornecedor. O comprometimento de contas de e-mail (EAC) pode ser utilizado em uma ampla variedade de ataques, mas é uma tática de impostura especialmente poderosa. As razões para isso são:

- A maioria das organizações não submete os e-mails internos aos mesmos níveis de escrutínio que os e-mails externos
- A maioria dos usuários confia intrinsecamente em e-mails de pessoas conhecidas
- Os atacantes que assumem o controle de uma conta têm acesso a inúmeras informações sobre o usuário comprometido — com quem ele se corresponde, o que discute e até mesmo sua forma de escrever. Esses detalhes tornam a impostura particularmente convincente.

A proteção de usuários internos, bem como contexto sobre risco de fornecedor, é essencial para uma segurança de e-mail eficaz.

## Torne os usuários mais resilientes com treinamento para conscientização quanto à segurança

Os atacantes cibernéticos tornaram-se implacavelmente eficazes na exploração da natureza humana com técnicas convincentes de falsificação, linhas de assunto que chamam a atenção e chamadas a ação irresistíveis. Muitos desses e-mails não são clicados apenas pelo destinatário, mas encaminhados e clicados por outras pessoas.

O treinamento para conscientização quanto à segurança — especialmente como espinha dorsal de uma cultura de segurança generalizada — pode contribuir muito para fazer dos usuários uma última linha de defesa forte. Porém, é preciso que ele seja direcionado, contínuo e oportuno para ter impacto sobre os usuários. Um treinamento genérico anual não basta para mudar comportamentos ou construir uma cultura de segurança.

Tags de e-mail, que dão aos usuários indicações contextuais sobre a natureza da mensagem, também podem ajudá-los a identificar e a denunciar ameaças potenciais. Por exemplo, uma tag que informa ao usuário que o e-mail vem de um endereço externo ou que o domínio do e-mail é estranhamente semelhante ao de uma marca confiável pode ajudar a identificar um possível phishing.

O isolamento da Web e do e-mail é um outro controle que pode ser aplicado para conter e examinar automaticamente cliques de mensagens que podem levar a sites de credenciais falsas, anexos maliciosos ou URLs que contenham malware ou outras ameaças. Isso pode ser aplicado aos seus usuários mais expostos a risco, VIPs ou uma população mais ampla de usuários com base no risco.

**US$ 15,4 milhões**

Em danos por organização em 2021.

## Proteja dados contra violações e ameaças internas

Nenhuma defesa de e-mail pode deter todas as ameaças. Mesmo em uma força de trabalho das mais bem treinadas, alguns usuários podem se deixar enganar por ataques direcionados de engenharia social.

É por isso que toda defesa de e-mail deve incluir ferramentas de prevenção de perda de dados (DLP), inclusive criptografia. Mesmo quando algo vai mal, uma resposta rápida e DLP asseguram que o ataque não se espalhe e que os atacantes não acessem os seus dados mais confidenciais.

A DLP também é uma defesa útil contra ameaças internas. Ninguém gosta de pensar que colegas de trabalho podem ser inimigos em termos de segurança. Porém, ameaças internas — as quais incluem funcionários descuidados, criminosos ou comprometidos — causaram uma média de US$ 15,4 milhões em danos por organização em 2021.[14]

Seja como for, se os dados saem do seu ambiente por meio de uma violação externa ou de um ataque interno, A DLP ajuda a mantê-los seguros.

14 Ponemon Institute. "2022 Cost of Insider Threats Global Report" (Relatório global sobre o custo das ameaças internas de 2022). Janeiro de 2022.

# Camada adaptável: controles adaptáveis para usuários mais arriscados

Uma proteção centrada em pessoas bem desenvolvida reconhece que alguns usuários precisam de controles e camadas de segurança adicionais. Tais usuários podem estar mais sujeitos a serem vítimas de ataques. Eles podem ser mais visados pelos ataques. Eles podem ter altos privilégios de usuário em relação a sistemas e dados confidenciais. Ou podem ter alguma combinação desses três fatores que resulte em um risco geral mais elevado.

**Estes são controles essenciais para usuários mais arriscados:**

- Treinamento direcionado para conscientização quanto à segurança
- Proteções adaptáveis com base no risco, como autenticação adicional e isolamento da Web e de URLs
- Proteções contra comprometimento (sequestro) de contas baseadas na nuvem

## Treinamento direcionado para conscientização quanto à segurança

O treinamento para conscientização quanto à segurança no âmbito da empresa é útil para revelar vulnerabilidades e reduzir a sua superfície de ataque humana. Além de corrigir deficiências óbvias, o treinamento direcionado também pode ser uma medida preventiva útil para todos os usuários sob risco e não apenas aqueles com níveis elevados do componente vulnerabilidade.

Usuários que representam um risco maior devido a seu perfil de ataque, por exemplo, podem obter treinamento exatamente sobre as ameaças que os estão visando. Usuários com altos privilégios podem obter treinamento extra relacionado a campanhas de ataque voltadas contra os dados aos quais eles têm acesso.

## Controles adaptáveis com base no risco

Aplicar os controles de segurança mais rígidos a todos os usuários ao mesmo tempo não é algo prático para a maioria das organizações. Pode até mesmo ser contraproducente. Controles desnecessariamente rigorosos podem afetar a produtividade dos usuários e levá-los a contornar as medidas de segurança, apenas para fazer seu trabalho.

Às vezes, porém, essa camada extra de segurança é necessária. Um funcionário da linha de frente pode estar particularmente exposto a um ataque que esteja circulando no seu setor. Um pesquisador pode ser visado por um atacante especialmente sofisticado. Ou um CEO, devido à natureza de seu trabalho, pode ter acesso aos dados mais confidenciais da organização.

Em alguns casos, pode ser necessário aumentar os requisitos de autenticação. Em outros, talvez seja preciso utilizar isolamento de Web para quaisquer URLs nos quais o usuário clique em um e-mail.

Seja qual for sua forma, a chave das proteções adaptáveis é ter uma boa noção dos fatores de risco relacionados às VAPs e aplicar controles proporcionais a esses riscos.

## Proteções para contas baseadas na nuvem

Para um criminoso cibernético, uma conta comprometida é praticamente uma licença para roubar.

Uma conta comprometida pode ser utilizada de inúmeras maneiras maliciosas. Ao obter controle sobre o acesso do usuário certo, o intruso pode se movimentar lateralmente dentro do seu ambiente, roubar dados ou enganar os seus clientes e parceiros comerciais. É por isso que a proteção de contas de e-mail, especialmente contas baseadas na nuvem, é fundamental.

# Camada de resposta: deter ameaças mais rapidamente e com mais eficiência

Incidentes de segurança são inevitáveis. Porém, eles não precisam ser catastróficos.

Quando um ataque consegue penetrar as defesas, a rapidez com que você pode conter e remediar os danos pode significar a diferença entre um incidente breve e uma incapacitação duradoura. Por isso uma estrutura de resposta vigorosa é parte essencial de toda postura de segurança centrada em pessoas.

**Em muitas organizações, a resposta a incidentes pode ser um processo lento e trabalhoso que inclui:**

- Investigação e verificação do incidente
- Quarentena de e-mails inseguros
- Contenção da ameaça
- Determinação da causa e do alcance
- Remediação dos sistemas infectados

Todas essas etapas são críticas para uma resposta eficaz. No entanto, como bem sabem os líderes de segurança, realizá-las manualmente não é viável em grande escala. Nisso a automação pode ajudar.

Processos de resposta eficazes automatizam tarefas trabalhosas, como correlacionar e analisar alertas de segurança, verificar indicadores de comprometimento (IOCs) e coletar dados forenses. A automação também pode ajudar em trabalhos de remediação, como atualização de listas de bloqueio de e-mail e firewall, remoção de e-mails maliciosos das caixas de entrada e restrição de acesso às contas dos usuários afetados.

Utilizada estrategicamente, a automação acelera a sua resposta a incidentes e libera o seu pessoal de segurança para se concentrar nas coisas que seres humanos fazem melhor. Em vez de serem reativos diante de uma avalanche de ameaças, eles podem aplicar medidas de proteção proativas.

# Como a inteligência artificial e a autoaprendizagem podem ajudar

Os atacantes visam pessoas. Eles exploram pessoas. E, no final da contas, eles também são pessoas.

Para detê-los são necessárias soluções modernas que possam se adaptar à forma como os seres humanos agem. Por isso a autoaprendizagem é um componente crítico em qualquer estratégia de segurança centrada em pessoas.

A autoaprendizagem é mais rápida e mais eficaz que a análise manual humana. E, diferentemente de algoritmos tradicionais, baseados em regras, ela pode se adaptar rapidamente a ameaças e tendências novas e em evolução.

## Autoaprendizagem versus BEC

Usemos o BEC como exemplo. Ataques de fraude de fatura de fornecedor por BEC são esquemas sofisticados e complexos concebidos para roubar dinheiro. Eles atuam apresentando uma fatura fraudulenta como se fosse legítima ou redirecionando o pagamento para uma conta bancária controlada pelo atacante.

As ferramentas de segurança tradicionais têm dificuldades com esse tipo de ataque devido a dois fatores: tais ataques são altamente direcionados e não contêm cargas virais. A autoaprendizagem pode analisar uma ampla variedade de atributos da mensagem — inclusive informações de cabeçalho, domínio e corpo da mensagem — para detectar uma mensagem impostora ou um fornecedor comprometido.

## Análise do phishing de credenciais

Os ataques de phishing de credenciais são um outro exemplo. Esses ataques de engenharia social costumam utilizar sites derivados nos quais as vítimas são induzidas a digitar suas credenciais. Frequentemente eles são tão bem desenvolvidos que os visitantes humanos não conseguem distingui-los dos originais. No entanto, com o uso de autoaprendizagem e visão de computador para examinar e analisar URLs rapidamente, as ferramentas de segurança modernas podem identificar e bloquear quaisquer e-mails que apontem para os sites falsos. A autoaprendizagem pode detectar URLs arriscados, mesmo que estes tenham sido registrados recentemente, estejam sendo hospedados por sites de compartilhamento de arquivos ou utilizem técnicas avançadas de evasão, como CAPTCHA.

## Se entra lixo, sai lixo

Diferentemente de sistemas de software padrão baseados em regras, o comportamento da autoaprendizagem é derivado dos dados e não predefinido. Isso significa que os sistemas de autoaprendizagem não podem ser melhores que as pessoas que os treinam ou que os dados utilizados.

Ao avaliar fornecedores que exaltam seus recursos de autoaprendizagem, procure modelos baseados em autoaprendizagem treinados com grandes conjuntos de dados de ameaças. Os dados devem incluir insights sobre ameaças obtidos de grandes corporações da Fortune 100, Fortune 1000 e Fortune Global 2000 e tantos provedores de serviços de Internet e pequenas e médias empresas quanto possível. Tais dados devem abranger múltiplos vetores de ataque, como e-mail, nuvem, rede e mídias sociais. Esses canais são críticos, pois os atacantes complementam seu arsenal indo além das ameaças baseadas em e-mail.

Não se esqueça do papel desempenhado por pesquisadores de ameaças habilidosos no treinamento de modelos de autoaprendizagem. Nem mesmo os melhores cientistas de dados podem construir sozinhos um modelo de autoaprendizagem eficaz. Eles precisam do conhecimento específico associado a uma base sólida em pesquisa e análise de ameaças.

LISTA DE VERIFICAÇÃO

# O que procurar em uma solução de segurança

A segurança centrada em pessoas é mais que um jargão de marketing — é uma maneira fundamentalmente nova de encarar as ameaças e de como detê-las. Ela começa com a abordagem certa, mas também exige ferramentas e capacidades.

Segue uma lista do que exigir em soluções de segurança centradas em pessoas.

## Uma plataforma unificada, integrada e expansível

Uma solução de segurança centrada em pessoas é mais do que a soma de suas partes. Soluções individuais podem resolver alguns aspectos do seu problema de segurança. Porém, combater ameaças modernas requer uma abordagem holística e integrada que considere cada tática, ferramenta e vetor que os atacantes utilizam — em cada dispositivo, plataforma e canal que o seu pessoal utiliza.

Produtos de segurança não integrados e com múltiplos consoles significam mais tempo e recursos desperdiçados com fluxos de trabalho redundantes e complicados. As equipes de segurança ficam com uma visão fragmentada das ameaças, um trabalho que as ocupa demasiadamente e mais complexidade no gerenciamento.

Procure soluções que cubram uma ampla variedade de ameaças e que trabalhem com o seu ecossistema de segurança mais amplo. Dependendo da sua organização, isso pode incluir componentes tais como firewalls de última geração, gerenciamento de eventos e informações de segurança (SIEM) e ferramentas de gerenciamento de identidade.

## Segurança eficaz para todos os usuários

A melhor maneira de frustrar ataques de e-mail é adotar uma abordagem em camadas, há muito recomendada pela Gartner e outros especialistas.

**Certifique-se de que suas defesas cibernéticas possam mitigar:**

- Spam e e-mail em massa indesejado
- Ataques que utilizam URLs e anexos maliciosos
- Ataques sem carga viral, como BEC
- EAC e sequestros de contas na nuvem

As pessoas desempenham o papel principal nos atuais ataques de e-mail. É por isso que o treinamento para conscientização quanto à segurança deve ser parte fundamental da sua estratégia de segurança de e-mail. Certifique-se de que o seu programa de treinamento inclua o seguinte:

- Treinamento em módulos pequenos de fácil assimilação para assegurar uma boa interação e mudança comportamental
- Simulações de phishing modeladas com base em campanhas do mundo real para treinar os usuários a lidar com as ameaças mais prováveis
- Instrução contínua, orientada por dados, para usuários vulneráveis visados por atacantes ou que interagem com mensagens de phishing reais
- Tags de e-mail que alertem os usuários a ter cuidado com mensagens suspeitas, com mecanismos internos de geração de relatórios e feedback para usuários

Para proteger dados roubados, compartilhados inadvertidamente ou expostos maliciosamente por um elemento interno, criptografia e outras medidas de prevenção de perda de dados (DLP) são fundamentais. Uma DLP eficaz pode:

- Analisar e classificar o conteúdo detalhadamente e, quando necessário, impedir que ele seja enviado por e-mail, transferido para a nuvem ou carregado em um dispositivo USB
- Identificar usuários maliciosos, negligentes ou comprometidos e ajudar as equipes de TI, de RH, do departamento jurídico e de segurança a executar as ações apropriadas para prevenir danos duradouros
- Identificar e proteger todas as formas padrão de conteúdo restrito, como PCI, HIPAA, FINRA e outros materiais regulamentados
- Redirecionar, criptografar ou rejeitar automaticamente e-mails que violem políticas de segurança ou outras políticas e alertar as pessoas apropriadas dentro da sua organização

## Controles adaptáveis para usuários mais arriscados

Usuários de risco mais alto — com base em sua vulnerabilidade, perfil de ataque e privilégio — precisam de controles de segurança adicionais. Uma solução de segurança de e-mail centrada em pessoas ajuda você a identificar essas VAPs e a protegê-las com camadas de segurança adicionais. Procure uma solução que:

- Ofereça visibilidade decisiva sobre suas VAPs. Informada por uma inteligência contra ameaças detalhada e atualizada, bem como insights profundos sobre os perfis de risco dos usuários
- Ofereça ferramentas de geração de relatórios que tornem fácil revelar e comunicar a vulnerabilidade, o perfil de ataque e o privilégio dos usuários, com comparações por departamento e por setor
- Responda automaticamente a perfis variáveis de risco de usuário com autenticação adicional, redução de privilégios, isolamento de URLs e mais

## Resposta fácil e eficaz quando algo passa pelas defesas

A automação de partes fundamentais do processo de resposta a incidentes pode ajudar a simplificar tarefas trabalhosas críticas e liberar os responsáveis pela resposta para atividades de nível mais alto. Procure ferramentas de resposta automatizada que:

- Verifiquem ameaças, identifiquem os usuários afetados e coletem dados forenses e o contexto em torno desses usuários
- Enriqueçam os alertas de ameaças com inteligência decisiva
- Contenham e remediem ameaças por todo o ambiente, na nuvem e no local. As ações corretivas automatizadas podem incluir análise de e-mails denunciados por usuários, remoção de ameaças verificadas de e-mails das caixas de entrada dos usuários e redefinição de senhas de contas comprometidas

## SAIBA MAIS

Para obter mais informações, visite www.mailsecurity.com.br

---

**MAILSECURITY PROTECTION**
The E-mails Security Experts

**SOBRE A MAILSECURITY PROTECTION**

A MailSecurity Protection, é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a MailSecurity ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos.

Organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, contam com a MailSecurity para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em **www.mailsecurity.com.br**.