proofpoint.

EBOOK

2022

The Definitive Email Cybersecurity Strategy Guide

A people-centric approach to stopping ransomware, malware attacks, phishing and email fraud

Email: Your Most Critical Threat Vector

Every day around the world, a silent battle wages on in one of the most familiar and central features of modern work: the email inbox.

As the top malware delivery vector and fertile ground for all kinds of fraud, email is the channel where cyber attackers are most likely to compromise their targets. They trick users into clicking on an unsafe link, giving away their credentials, or even carrying out commands directly (such as wiring money or sending sensitive files).

It's not hard to see why attackers prefer email. It uses a decades-old architecture that wasn't designed with security in mind. It's universal. And unlike computer hardware and infrastructure, email attacks exploit vulnerabilities that can't be patched: people.

The challenge is growing even more complicated amid a shift to the cloud and remote work.

Organizations spend billions every year on security tools designed to harden the network perimeter, detect network intrusions and secure endpoints. And yet the volume—and costs—of ransomware, business email compromise (BEC), credential phishing and malware-fueled data breaches have never been higher.[1]

That's because today's attacks hack human nature, not just technology. And email is the easiest way to reach people.

Consider these research findings:

$14.8 million
the average annual costs of phishing for a large organization—more than triple the 2015 average[2]

86%
of organizations faced bulk phishing attacks in 2021[3]

77%
of organizations faced BEC attacks in 2021[4]

78%
of organizations saw email-based ransomware attacks in 2021[5]

85%
of data breaches involve people[6]

1 Ponemon. "The 2021 Cost of Phishing Study." June 2021.
2 Ponemon. "The 2021 Cost of Phishing Study." June 2021.
3 Proofpoint. "2022 State of the Phish." February 2022.
4 Ibid.
5 Ibid.
6 Verizon. "Data Breach Investigations Report Executive Summary." May 2021.

It's time for a new approach. Today's threat landscape calls for a fresh mindset and new strategy—one that focuses on protecting people rather than infrastructure.

Whether you lead a multinational security operations center or a small tight-knit security team, consider this guide a starting point. We'll explore:

- Why email should be your No. 1 security priority
- What makes it so difficult to secure
- How integrated, layered people-centric security is more effective
- Where to optimize your email security operations to save money and streamline response

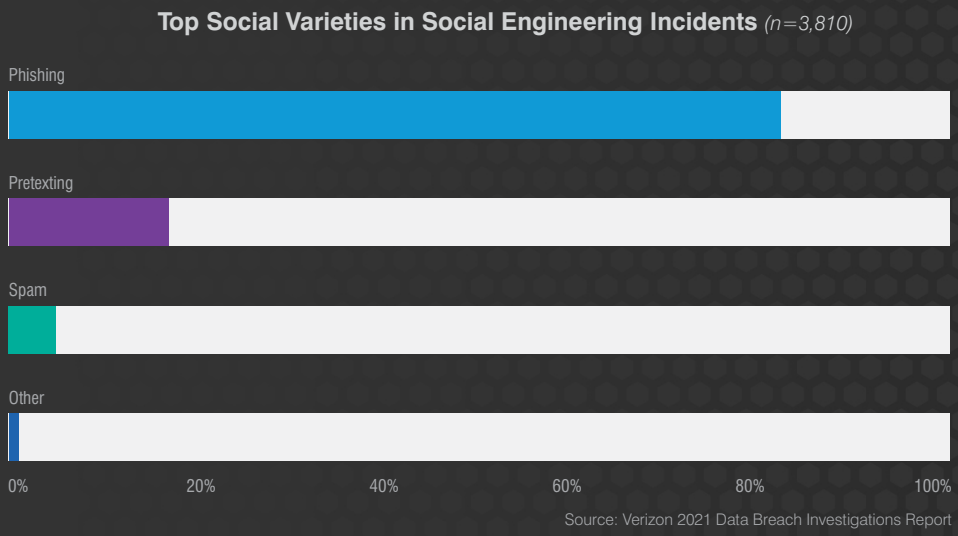


Figure 1: Top forms of social engineering

SECTION 1

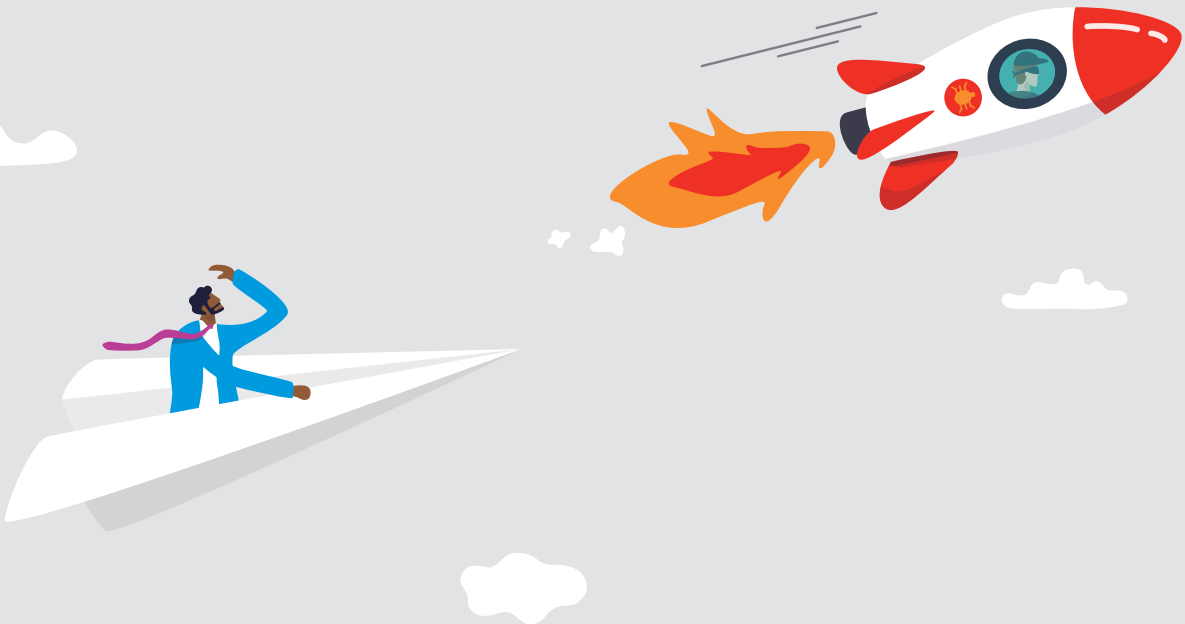
Cyber Attacks Are Evolving Faster Than Traditional Defenses

Safeguarding email is the key to protecting the enterprise. But it's a complex challenge.

That's because email threats are numerous and wide-ranging. Attack techniques are constantly evolving. And human nature—the weak link in every organization—is a perpetual target.

It's no wonder that solutions built for fighting the attacks of just two to three years ago are struggling to keep up.

This section outlines just some of the ways cyber attackers target people. (In many cases, attackers combine techniques to evade defenses and boost their success rates.)



Ransomware

Ransomware is an old threat that persists as a modern-day problem. This type of malware—which gets its name from the payment it demands after locking away victims' files—is a major issue for modern businesses. It's one of today's most disruptive types of cyber attack.

Major incidents involving fuel,[7] food[8] and health infrastructure[9] in 2021 showed that no target is off limits.

About three-quarters of ransomware starts, directly or indirectly, with a phishing email.[10] These emails trick users into opening a malicious attachment or clicking a malicious URL.

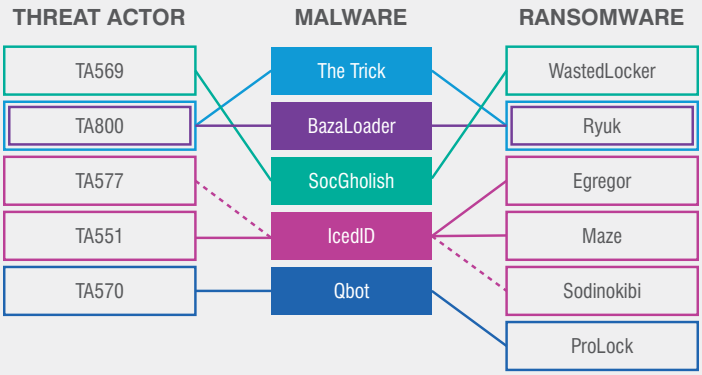


Figure 2: Links between threat actors, first-stage malware and ransomware

Most ransomware is delivered as a secondary infection after a system is already infected with a Trojan or loader. Many attackers who specialize in these Trojans or loaders then sell access to ransomware organizations. For most organizations, the first line of defense against ransomware is making sure they are protected from other kinds of malware.

There isn't a simple one-to-one relationship between the initial access malware and the strain of ransomware distributed to victims. But researchers at Proofpoint and elsewhere in the industry have noted some prominent associations, as shown in Figure 2.

7 David Sanger, Clifford Krauss, Nicole Perlroth (New York Times) "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." May 2021.
8 Julie Creswell, Nicole Perlroth, Noam Schreiber (New York Times) "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business." June 2021.
9 Nicole Perlroth, Adam Satariano (New York Times) "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks." May 2021.
10 Unit 42, Palo Alto Networks. "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report." July 2021

Email fraud and business email compromise (BEC)

Business email compromise (BEC), also known as email fraud, is one of cybersecurity's costliest and least understood threats. The fast-growing category of email fraud doesn't always garner as much attention as other high-profile cyber crimes. But in terms of direct financial costs, BEC easily overshadows other types.

In 2020 alone, BEC schemes cost organizations and individuals more than $1.8 billion.[11] That's up more than $100 million from 2019 and a full 44% of total cyber crime losses.

BEC attacks are hard to detect. They don't include the usual payloads—malicious URLs or file attachments—to analyze. Instead, fraudsters rely on impersonation and other social engineering techniques to trick people.

Many of today's BEC schemes are highly sophisticated, well-funded and backed by careful planning and research. A growing number of attackers are focusing their efforts on supplier invoicing fraud and large business-to-business (B2B) transactions they can hijack.

BEC attacks prey on human nature. They exploit people's trust.

Here's how they work:

1. First, BEC attackers pose as a person or entity that a recipient can trust, such as a colleague, boss or vendor.
2. The attacker sends an email directing recipients to take some action that siphons money or sensitive financial information from the organization. These could include fraudulent wire transfers, bogus invoices, diverted paychecks, changed banking details for future payments, and countless other schemes.
3. By the time the organization discovers the error, it's often too late to recover the money.

TYPES OF BEC

BEC comes in many forms—limited only by attackers' creativity. Here are six common types:

1. **Invoicing fraud.** This attack tricks victims into paying bogus invoices or diverting valid payments.
2. **Payroll redirect.** In this scheme, attackers posing as an employee ask the payroll department to reroute wages to their account.
3. **Extortion.** Here, attackers threaten harm or embarrassment unless the victim pays up.
4. **Lures and tasks.** These bait victims with a simple question like "Are you there?" and escalate to other forms of BEC.
5. **Gift carding.** This technique tricks recipients into buying gift cards and sending the number and PIN to the scammer.
6. **Advance-fee fraud.** In this old con, swindlers ask for money to unlock an even larger sum—which never comes.

11 FBI. "Internet Crime Report 2020." March 2021.

Account compromise/takeover

Account compromise is the act of maliciously gaining control over a legitimate user's email or cloud service account—giving the attacker wide-ranging access to data, contacts, calendar entries and email.

Beyond the compromised user's data, the attacker can use the account to impersonate the user in social engineering attacks both inside and outside of the organization. These include BEC, supply-chain attacks and more.

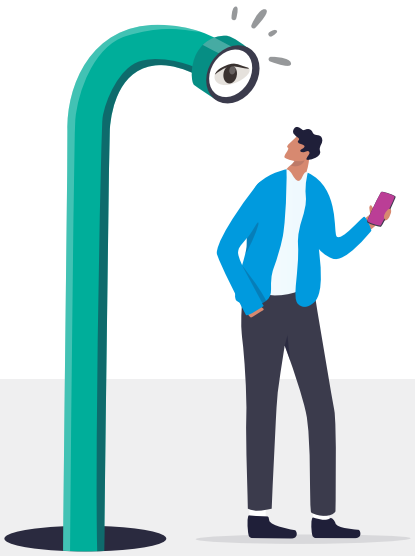
Threat actors can access sensitive data, persuade users or outside business partners to wire money or damage an organization's reputation and finances. Worse, they can also install backdoors to maintain access for future attacks.

Anatomy of an account takeover

Here's how most cloud account takeovers play out.

Credential theft. The attacker gains access to the user's credentials through credential phishing (which alone accounts for about two-thirds of all phishing volume), brute-force password attacks, credential restuffing/recycling or credential-stealing malware.

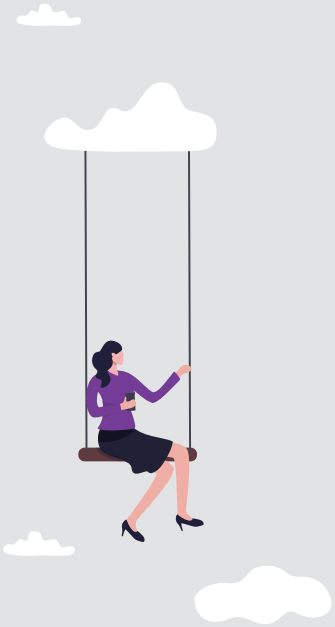
Infiltration. Once logged into the user's account, the attacker has access to the victim's email, contacts, calendar and files. The attacker can steal this data directly or use it to convincingly impersonate the user. Some fraudsters may respond to existing email threads or send draft emails with malware or unsafe URLs to colleagues and outside business partners. Posing as the compromised users, other may target others inside and outside the company with fake invoices or payment rerouting instructions. The attacker may also upload malware into corporate file-shares or sabotage the company in other ways.



Persistence. Often, the attacker stealthily sets up auto-forwarding rules that provides access to the user's email even if the user changes the password. Being able to see all incoming email and calendar invites gives the attack key details for future impersonation attacks.

SECTION 2

How the Threat Landscape Has Changed

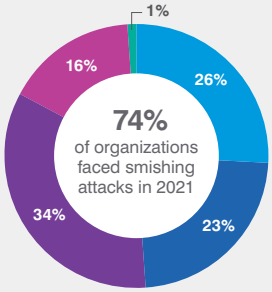


Today's remote and hybrid workforces are powered by cloud and mobile technologies.

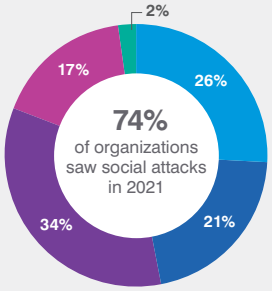
The hardened perimeters and traditional network structures of the past are all but gone. People are the new perimeter.

Unfortunately, most security budgets—tied to other priorities and product categories—haven't kept up.

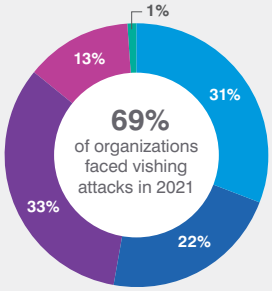
Volume of Smishing Attacks



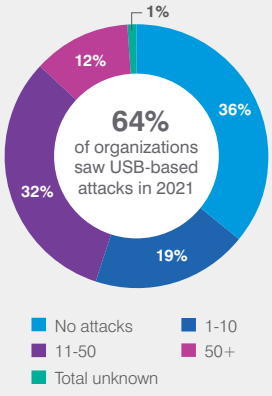
Volume of Social Media Attacks



Volume of Vishing



Volume of Malicious USB Drops



Source: 2022 State of the Phish

Attackers target people, not infrastructure

Even as organizations spend billions every year to shore up their infrastructure, they may be neglecting the people-based security risks that matter most. People are the easiest and most lucrative entry point into your environment.

According to the "Verizon Data Breach Investigations Report," a whopping 85% of data breaches involve people.[12] Your users are under a constant barrage of unsafe hyperlinks, malicious attachments, credential theft, social engineering schemes and impostor threats.

Attacks often span multiple vectors

Targeting people means engaging them on the tools and platforms they use. Where users go, attackers follow.

Modern workflows are dynamic and unpredictable. User may start a conversation in email, schedule a follow-up meeting in their chat application and collaborate on files stored in the cloud.

Modern attacks are also dynamic and unpredictable. They play out over multiple channels, use a mix of tactics and tools and piggyback all the platforms people use to get their work done.

An attack may start with email and link to malware hosted on a file-sharing site. Or a rogue cloud app may steal credentials to compromise a legitimate account and use it to launch BEC attacks.

The challenge is only growing. Often, an advanced threat actor creates the malware "product" and sets up the infrastructure as an easy-to-use package or service. Lower-level cyber criminals may rent the service for their attacks, paying to use it for a set period of time or getting a cut for each successful compromise. In other cases, they act as distributors, sending out emails with the malware and earning a commission on each successful infection.

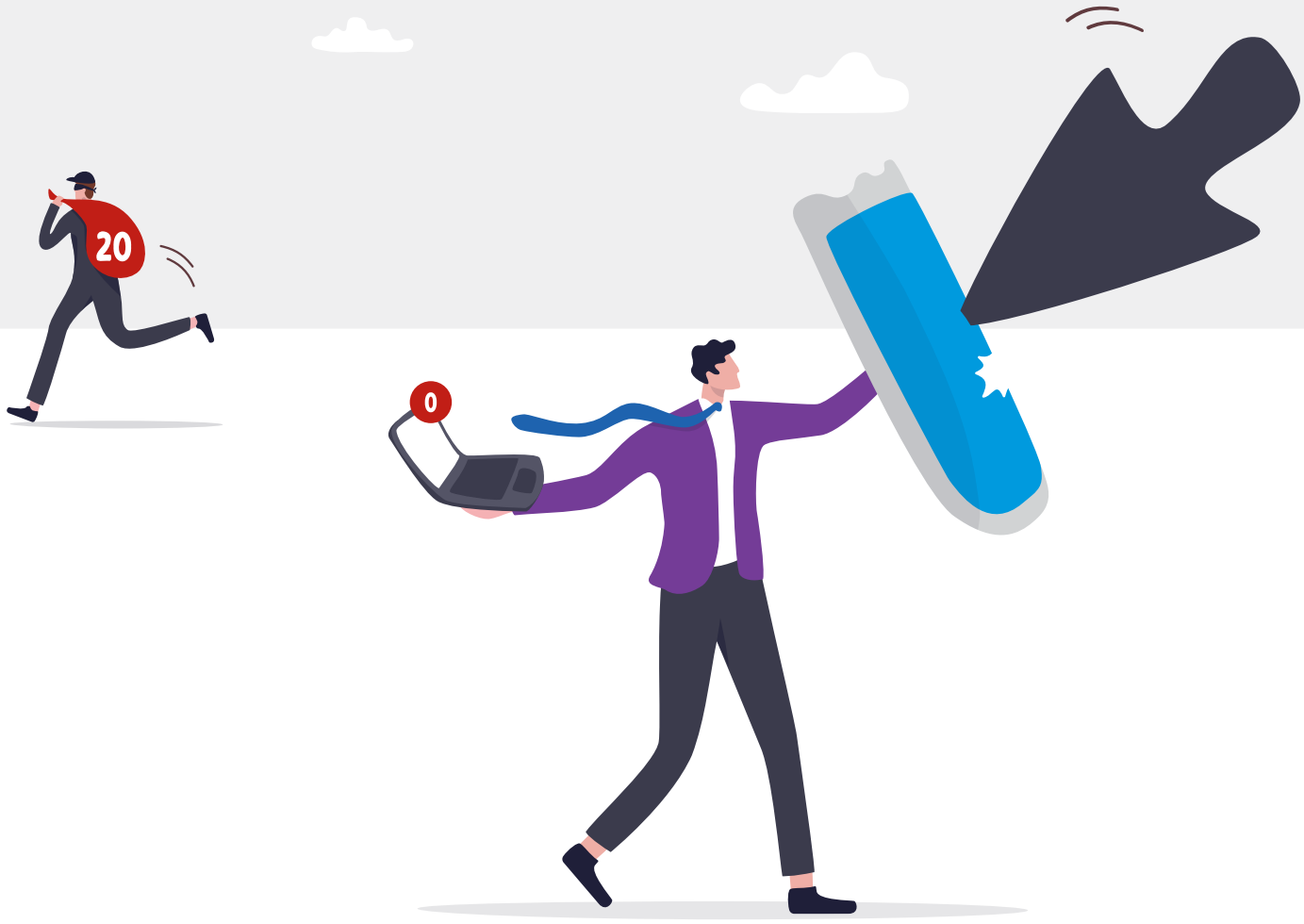
12 Verizon. "Data Breach Investigations Report Executive Summary." May 2021.

Defending every vector is not enough

Organizations may understand the multifaceted, people-centric nature of today's threats and invest in security tools to cover every potential risk. But unless those tools are working together in a coordinated fashion, they can't offer the visibility and insight security teams need to manage risk.

Imagine a squad of soccer superstars who won't practice together, an orchestra of virtuosos who don't hear the other instruments, or a surgical team that can't agree on patient care. No matter how skilled each individual is, they're not nearly as effective a well-coordinated whole.

Today's attackers combine techniques for more sophisticated attacks. Standalone point products tools create needless complexity for security teams struggling to just to manage the current risk. That's why true people-centric security requires a holistic, coordinated approach.



SECTION 3

Focus on Your Riskiest Users

The first step to protecting users is identifying which ones pose the most risk. While every organization may weigh various risk factors differently, all should comprise some combination of vulnerability, attacks and privilege.

Vulnerability is a way of determining who's most likely to fall victim to a threat. An attack analysis can reveal who in your organization is being targeted, how heavily and by what types of threats. And privilege can help predict how harmful a successful attack would be to the organization.

Focus on users who represent a higher-than-normal risk based on any combination of these factors. Their status calls for extra attention by the security team and stakeholders who should know how and why they're at risk.

This level of visibility in all three areas is essential to people-centric security. Without it, organizations have no way of knowing who needs additional layers of security or how best to protect them.

Vulnerability: how people work and what they click

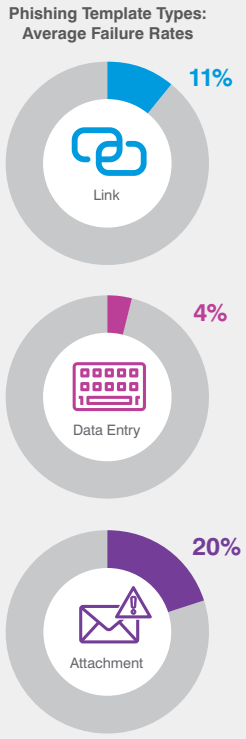
Quantifying vulnerability isn't easy with traditional technology-focused security tools. But with a people-centric approach, you can measure: how they work and what they click. How they work encompasses the tools, systems and platforms they use to do their job. What they click is a measure of their security awareness and propensity to fall for likely threat tactics.

How your people work

You can get a general sense of user vulnerability by assessing what tools, platforms and apps they use. These may include:

- What cloud apps they use and whether those apps are vetted by the IT department
- How many and what devices they use to access email
- Whether those devices are secure
- Whether the user practices good digital hygiene such as strong, unique passwords and keeping software up to date
- Whether they use multifactor authentication consistently for corporate access and even personal accounts

The more granular your visibility, the better.



Source: 2022 State of the Phish

What your people click

Vulnerability can be measured more precisely with security education, simulated phishing and how they respond to actual threats.

Security awareness training, an essential layer of any effective security strategy, can offer insight into which users are the least prepared to recognize, resist and report cyber threats. In general, users who score poorly on training exercises—or haven't completed them—are more vulnerable than high scorers.

Short of letting attackers in and seeing who clicks a link, fills out a form or opens a file, phishing simulations are one of the most powerful ways to gauge this aspect of vulnerability.

Finally, and most importantly, track users who engage with known malicious emails, even when the click is blocked, isolated or rewritten.

This real-world data combined with security awareness information gives you a holistic view into email vulnerability by tracking education completion, phishing simulations and engagements with real malicious messages.

Attacks: how people are targeted

Every cyber attack is potentially harmful. But some are more dangerous, targeted or sophisticated than others. That's why measuring this aspect of risk might be trickier than it seems.

Indiscriminate "commodity" threats might be more numerous than other kinds of threats. But they're well understood and more easily blocked.

Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

Knowing the difference is critical to identifying users who are a higher risk. At Proofpoint, we call these users "Very Attacked People™" (VAP). Having a complete view of all email traffic and tying this to rich threat intelligence are keys to quantifying who is being targeted and how heavily.

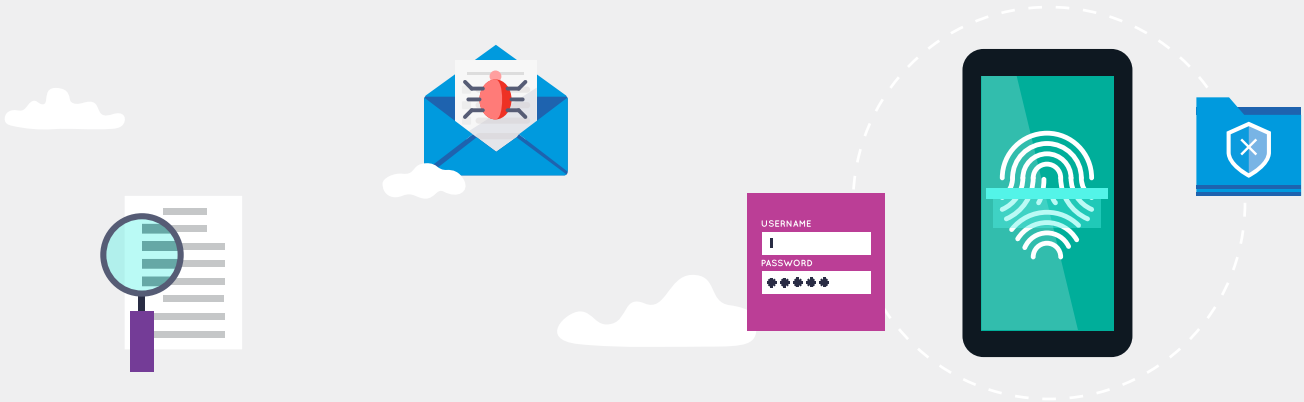
The factors that should weigh most heavily in each user's assessment include:

- The cyber criminal's sophistication
- The spread and focus of attacks
- The attack type
- Overall attack volume

You should also weigh these factors in context of what departments, groups or divisions the individual user belongs to.

For instance, some users might seem not at risk based on the volume or type of malicious email sent to them directly. But they may actually represent a higher risk because they work in a highly attacked department—and are therefore more likely to be a key target in the future.

Good threat intelligence can determine what tools attackers are using and tie seemingly discrete incidents to larger campaigns.



Privilege: what people have access to

Measuring user privilege starts with taking an inventory of all the potentially valuable things people have access to: data, financial authority, key relationships and more. You should know where your most sensitive data lives and who and what apps have access to it.

Users with access to critical systems or proprietary intellectual property, for instance, might need extra protection, even if they aren't especially vulnerable or aren't yet on attackers' radars.

The user's position in the org chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one.

An administrative assistant might make a more appealing target than a mid-level manager for corporate espionage because the assistant has access to the CEO's calendar. In the same way, a hospital nurse with access to patient records might be more useful target than the CEO for identify thieves.

For attackers, a valuable target can be anyone who serves as a means to their end.

Protecting high-privilege users from outside attacks is critical. Just as important is protecting your organization from high-privilege users. In the wrong hands, insider access might be misused through malice, negligence or compromise. Compromised accounts could export sensitive files or attempt to compromise or defraud other internal users.

SECTION 4

Building a People-Centric Defense

A people-centric approach keeps everyone protected by applying controls that correspond to their level of risk. And it works in a unified way across every platform people use, against every tactic attackers employ and within every threat vector that matters.

Base layer: security for everyone

Because email attacks come in many forms, you need a defense that stops the entire gamut of email threats, not just some of them.

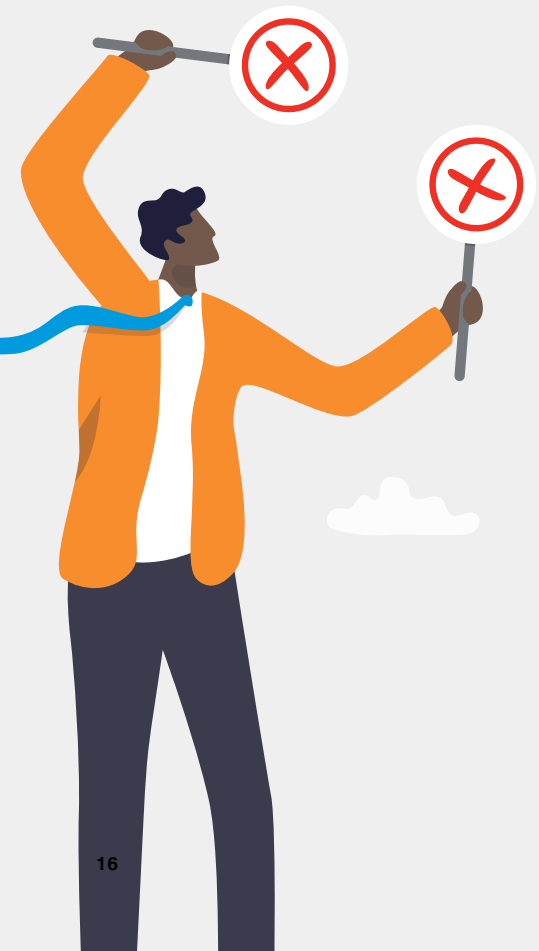
Here are the most essential steps to an email defense built for modern threats:

- Stop malicious attachments and URLs before they reach users' inboxes.
- Stop payload-free impostor threats such as BEC and other scams, including those coming from compromised email accounts within your own organization and from suppliers.
- Secure users' web browsing and personal email with web and personal email isolation.
- Make users more resilient with security awareness training and contextual clues.
- Apply controls such as web isolation to keep users' potential unsafe browsing habits separate from your environment.
- Factor data protection into to your email security strategy.

Stop malicious attachments and URLs before they reach users' inbox

Most cyber attacks rely on the intended victim doing something—in many cases, opening an attachment or clicking a URL. But these human-activated attacks can't succeed if the intended victim never sees the message.

That's where advanced email security protection comes in. By stopping malicious payloads before they reach users' inboxes, an effective solution can protect against a wide range of malware threats, including ransomware, banking Trojans, remote-access Trojans, information stealers, downloaders, botnets and more.



Stop hard-to-detect impostor threats

Stopping malware is critical, but some of the most damaging email attacks don't use payloads at all. Instead, they rely on social engineering.

BEC, a type of wire-transfer fraud, is one example. BEC attacks been reported in all 50 states and 177 countries, with fraudulent transfers sent to at least 140 countries, according to the FBI.[13]

In BEC and other forms of email fraud, the scammer impersonates someone the recipient can trust using a spoofed, compromised or lookalike email account. Under that false identity, the attacker asks the victim to do something on the attacker's behalf—say, wire money to an overseas bank account, send sensitive files and more.

Impostor threats are a complex problem with many facets. To stop them, you need a layered defense that secures inbound, outbound and internal email—and works in a holistic, cohesive way.

13 FBI. "Internet Crime Report 2020." March 2021.

Along with user education and other security controls described in this section, here are key elements of an impostor email defense.

DMARC

Deploy Domain-based Message Authentication, Reporting and Conformance (DMARC) email authentication. DMARC is an internet-wide policy that validates that the email sender is who they say they are and that they're authorized to send on the organization's behalf.

With DMARC, you get visibility into all the email being sent using your email domain, including trusted third-party senders such as Marketo, Salesforce and others. With this visibility, you can authorize all valid senders trying to send email on your behalf—and block anyone using your trusted domains to steal money or hurt your brand.

Dynamic classification

While DMARC can help stop threats that spoof your domain, attackers use other techniques to trick users. That's why another critical component of stopping non-malware threats is dynamically analyzing and classifying the content of the emails. This aspect of email security is all about parsing what's in the email, not just where it comes from. That's why you need email security that can look for telltale signs of fraud and block or further study anything that looks unsafe. Dynamic classification analyzes and manages email based on several factors, including:

- The email's header, IP address and sender reputation
- Machine learning-driven content analysis looking for reply-to pivots, words and phrases
- The relationship between the sender and recipient
- Context about sender, such as whether it appears to be impersonating a known supplier

Internal email defense and supplier risk insights

In some cases, attackers don't try to disguise their email address at all—they just take over a legitimate account at the organization or a supplier or partner. Email account compromise (EAC) can be used in a wide range of attacks, but it's especially potent impostor tactic. That's because:

- Most organizations don't subject internal to the same levels of scrutiny and security controls as external email
- Most users inherently trust email from people they know
- Attackers who take control over an account have access to a trove of information about the compromised user—who they correspond with, what they discuss and even their writing style. These details make the impersonation especially convincing.

Protecting internal users, as well as context about supplier risk, is essential to effective email security.

Make users more resilient with security awareness training

Cyber attackers have grown ruthlessly effective at exploiting human nature with convincing spoofing techniques, attention-grabbing subject lines and hard-to-resist calls to action. Many of these emails aren't clicked just by the recipient but forwarded and clicked by others.

Security awareness training—especially as the backbone of a pervasive security culture—can go a long way toward making users a strong last line of defense. But it has to be targeted, ongoing and timely to make an impact with users. Generic annual training won't move the needle in changing behavior or building a security culture.

Email tags that give users contextual clues about the nature of the message can also help them spot and report potential threats. For example, a tag that lets the user know that the email is coming from an external address or that the email domain is confusingly similar to that of a trusted brand can help them spot potential phishing.

Web and email isolation is another control that can be applied to automatically contain and scan clicks from messages that may lead to fake credential sites, malicious attachments or URLs that contain malware or other threats. This can be applied to your most at-risk users, VIPs or a broader user population based on risk.

$15.4M

in damage per organization in 2021.

Protect data from breaches and insider threats

No email defense can stop every threat. And even among the best-trained workforce, some users may fall for targeted social engineering attacks.

That's why every email defense should include data loss prevention (DLP) tools, including encryption. Even when something goes wrong, a fast response and DLP ensures that the attack doesn't spread and that attackers don't get your most sensitive data.

DLP is also a useful defense against insider threats. No one likes to think of their colleagues as a potential security foe. But insider threats—including workers who are careless, criminal or compromised—caused an average of $15.4 million in damage per organization in 2021.[14]

Whether data exits your environment through an external breach or insider attack, DLP helps keep it secure.

14 Ponemon. "2022 Cost of Insider Threats Global Report." January 2022.

Adaptive layer: adaptive controls for riskier users

A well-honed people-centered protection recognizes that some users need additional security layers and controls. These users may be more vulnerable to falling victim to attacks. They may be more heavily targeted in attacks. They may have high user privileges to sensitive data and systems. Or they may have any combination of the three that results in higher overall risk.

Here are essential controls for riskier users:

- Targeted security awareness training
- Adaptive, risk-based protections such as step-up authentication, web and URL isolation
- Compromise (takeover) protections for cloud-based accounts

Targeted security awareness training

Company-wide security awareness training is useful for revealing vulnerabilities and reducing your human attack surface. Beyond shoring up obvious gaps, targeted training can also be a helpful preventative measure for all risky users, not just those who rank high on the vulnerability component.

Users who pose a higher risk because of their attack profile, for instance, can get training on the very threats that are targeting them. And users with high privileges can get extra training related to attack campaigns targeting the data they have access to.

Adaptive, risk-based controls

Applying the most stringent security controls to all users all of the time just isn't practical for most organizations. It could even backfire. Needlessly tight controls can hinder users' productivity and might drive them to turn to security workarounds just to do their job.

But sometimes, that extra layer of security is necessary. A frontline worker might be especially prone to an attack making the rounds in your industry. A researcher might be targeted by an especially sophisticated attacker. Or a CEO, because of the nature of the job, might have access to the organization's most sensitive data.

In some cases, you may need to step up authentication requirements. In other cases, you may need to use web isolation for any URLs the user clicks from email.

Whatever form they take, the key to adaptive protections is a having a timely picture of the VAP-related risk factors and applying controls that are proportional to those risks.

Account protections for cloud-based accounts

To a cyber criminal, a compromised account is practically a license to steal.

A compromised account can be used in all sorts of malicious ways. By gaining control of the right user's access, the intruder can move laterally within your environment, steal data or dupe your business partners and customers. That's why protecting email accounts, especially cloud-based accounts, is critical.

Response layer: stopping threats faster and more efficiently

Security incidents are inevitable. But they don't have to be catastrophic.

When an attack gets through, how quickly you can contain and remediate the damage can mean the difference between a short- lived incident and long-lasting impairment. That's why a vigorous response framework is a key part of every people-centric security posture.

At many organizations, incident response can be a slow, labor-intensive process that includes:

- Investigating and verifying the incident
- Quarantining unsafe email
- Containing the threat
- Determining the cause and scope
- Remediating infected systems

All of these steps are critical to an effective response. But as security leaders know all too well, performing them manually doesn't scale. That's where automation can help.

Effective response processes automate labor-intensive tasks such as correlating and analyzing security alerts, verifying indicators of compromise (IOCs) and collecting forensic data. Automation can also help with remediation efforts such as updating firewall and email blocklists, pulling malicious email from inboxes, and restricting account access of affected users.

Used strategically, automation speeds up your incident response and frees up your security staff to focus on the things people do best. Rather than being reactive to an onslaught of threats, they can apply proactive protection measures.

How artificial intelligence and machine learning can help

Attackers target people. They exploit people. And ultimately, they are people.

Stopping them requires modern solutions that can adapt to the way humans act. That's why ML is a critical component in any people-centric security strategy.

ML is faster and more effective than manual human analysis. And unlike traditional rule-based algorithms, it can quickly adapt to new and evolving threats and trends.

ML vs. BEC

Take BEC as an example. BEC supplier invoicing fraud attacks are sophisticated and complex schemes to steal money. They work by either presenting a fraudulent invoice as legitimate or by re-routing the payment to a bank account controlled by the attacker.

Traditional security tools struggle with this type of attack due to two factors: such attacks are highly targeted and contain no payload. ML can dynamically analyze a wide range of message attributes—including header information, domain and message body— to detect an impostor message or compromised supplier.

Analyzing credential phishing

Credential phishing attacks are another example. These socially engineered attacks often use knockoff log-in sites to trick victims into entering their credentials. Often, they're so well designed that human viewers can't tell the difference. But using ML and computer vision to quickly scan and analyze URLs, modern security tools can spot and block any emails that point to the counterfeit sites. ML can detect risky URLs, even if they're newly-registered, are being hosted by file-sharing sites or use advanced evasion techniques like CAPTCHA.

Garbage in, garbage out

Unlike standard rule-based software systems, ML behavior is derived from data and is not hand-coded. That means ML systems are only as good as the people who train them and the data they use.

When evaluating vendors that tout their ML features, look for ML-based models trained with large sets of threat data. The data should include threat insight gleaned from leading enterprises in the Fortune 100, Fortune 1000 and Fortune Global 2000 and as many internet service providers and small and mid-size businesses as possible. And it should span multiple attack vectors such as email, cloud, network and social media. These channels are critical as attackers augment their arsenal beyond email-based threats.

And don't forget the role of skilled threat researchers in training ML models. Even the best data scientists can't build an effective ML model alone. They need the domain expertise that comes with having a deep background in threat research and analysis.

CHECKLIST

What to Look for in a Security Solution

People-centric security is more than a marketing buzz-word—it's a fundamentally new way of looking at threats and how to stop them. It starts with the right approach but also requires the tools and capabilities.

Here's a checklist of what to demand in people-centric security solutions.

A unified, integrated and scalable platform

A people-centric security solution is more than the sum of its parts. Point solutions may solve some aspects of your security problem. But combating modern threats requires a holistic, integrated approach that addresses every tactic, tool and vector attackers use—across every device, platform and channel your people use.

Unintegrated security products with multiple consoles means more time and resources wasted with overlapping and convoluted workflows. Security teams get a fragmented view of threats, needless busywork and more management complexity.

Look for solutions that cover a broad range of threats and work with your broader security ecosystem. Depending on your organization, these might include components such as next-generation firewalls, security information and event management (SIEM) and identity management tools.

Effective security for all users

The best way to thwart email attacks is to take a layered approach long recommended by Gartner and other experts.

Ensure you cyber defenses can mitigate:

- Spam and unwanted bulk mail
- Attacks that use malicious attachments and URLs
- Payload-free attacks such as BEC
- EAC and cloud-account takeovers

People play the biggest role in today's email attacks. That's why security awareness training should be a key part of your email security strategy. Make sure your training program includes the following:

- Bite-sized training to ensure engagement and behavior change
- Phishing simulations modeled on real-world campaigns to train users on the threats they're most likely to face
- Ongoing data-driven education for vulnerable users who are targeted by attackers or engage with real phishing messages
- Email tags that alert users to be careful with suspicious messages, with built-in reporting mechanisms and feedback to users

To secure data that is stolen, mistakenly shared or maliciously exposed by an insider, encryption and other DLP measures are critical. Effective DLP can:

- Analyze and classify content in detail and, when needed, block it from being sent through email, transferred to the cloud or loaded onto a USB device
- Identify malicious, negligent or compromised users and help IT, HR, legal and security teams take the appropriate action to prevent lasting harm
- Identify and protect all standard forms of restricted content, such as PCI, HIPAA, FINRA and other regulated material
- Automatically reroute, encrypt or reject emails that violate security and other policies and alert the appropriate people within your organization

Adaptive controls for riskier users

Higher-risk users—based on their vulnerability, attack profile and privilege—require additional security controls. A people-centric email security solution helps you identify those VAPs and protect them with extra layers of security. Look for a solution that:

- Gives you actionable visibility into your VAPs informed by rich, timely threat intelligence and deep insight into users' risk profiles
- Offers reporting tools that make it easy to surface and communicate users' vulnerability, attack profile and privilege, with departmental and industry comparisons
- Automatically responds to changing user risk profiles with step-up authentication, reduced privileges, URL isolation and more

Fast, effective response when something gets through

Automating key parts of the incident response process can help streamline critical labor-intensive tasks and free up responders for higher-level activities. Look for automated response tools that:

- Verify threats, identify affected users and collect forensics data and context around those users
- Enrich threat alerts with actionable intelligence
- Contain and remediate threats across the environment, in the cloud and on premises. Automated corrective actions may include analyzing user-reported emails, pulling verified threats from email from users' inboxes and resetting passwords of compromised accounts.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0301-001-01-03 03/22