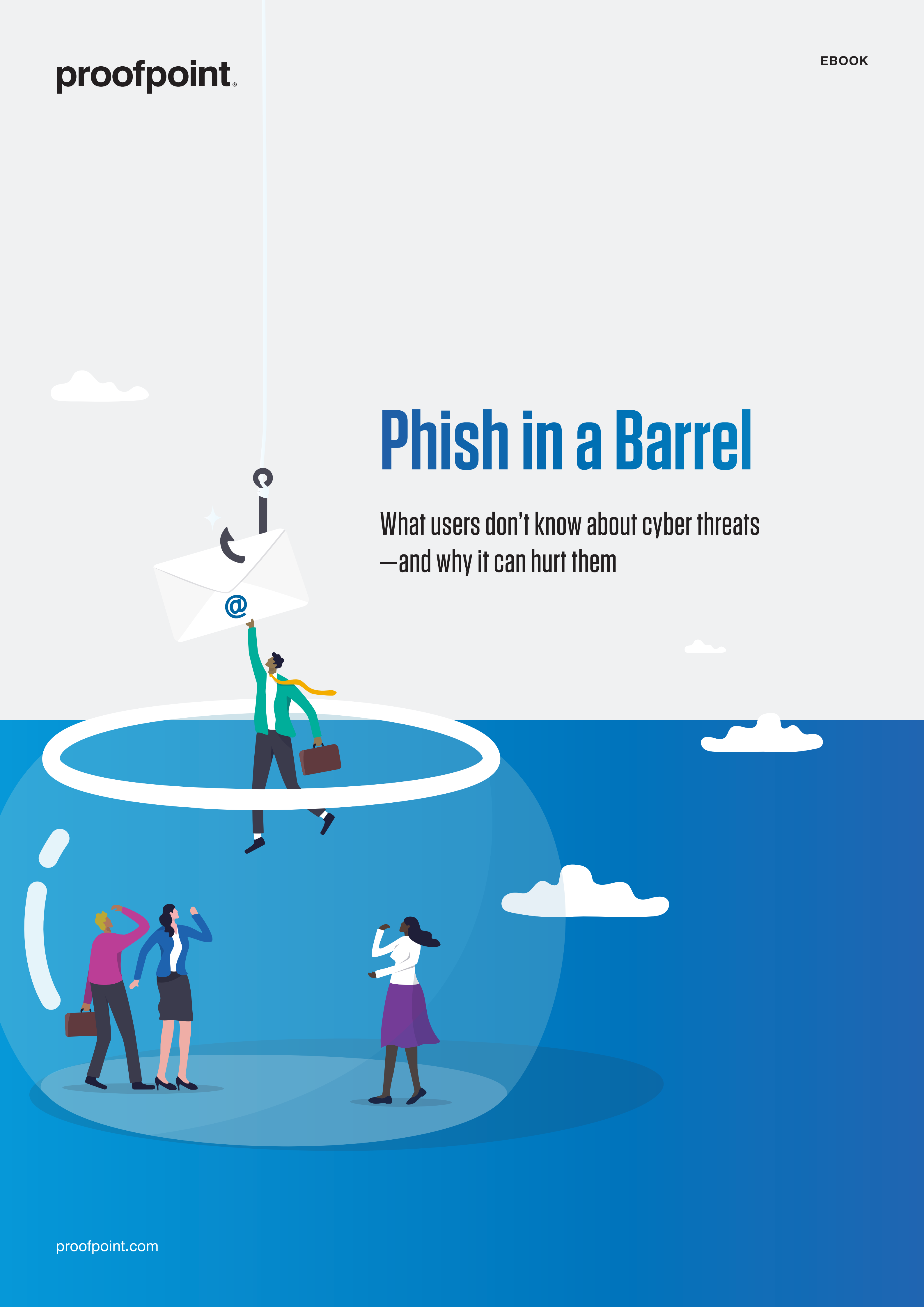
proofpoint.

EBOOK

Phish in a Barrel

What users don't know about cyber threats
—and why it can hurt them



proofpoint.com

Introduction

There's an old saying: *What you don't know can't hurt you*. But perhaps no statement could be less true when talking about cyber threats.

What your users don't know about cyber threats can hurt them—and your organisation. They're constantly being targeted by cyber attacks. Missteps caused by their lack of knowledge could lead to disruption, loss and long-term damage.

This e-book explores real-world attacks that reveal users' dual role as top targets for attackers and frontline defenders.

They span five major categories of cyber attacks and other cyber crime that began with—or hinged on—compromising users:

- Phishing
- Business email compromise (BEC)
- Ransomware
- Cloud attacks
- Web-based email attacks

We also include select findings from our [2022 State of the Phish]() report to highlight users' knowledge, vulnerabilities and resilience in these areas. The data has clear implications for security leaders looking to secure their users, data and brands. They also boldly underscore why people are the new perimeter—and therefore should be the focus of your cybersecurity efforts.

SECTION 1

Phishing

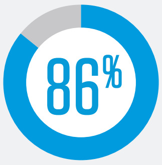
Phishing is a form of social engineering.

Delivered by email or text, phishing messages use a growing array of techniques to exploit human psychology. Threat actors takes advantage of users’ trust to get financial information, system credentials and other sensitive data.

Trends

With each passing year, phishing is becoming more of a go-to tool for attackers. According to the FBI's *2021 Internet Crime Report*, phishing and similar attacks accounted for more than 38% of all suspected internet crime reported in the United States last year. Nearly 323,000 phishing attempts were reported in 2021. That's nearly 83,000 more complaints than in 2020 and 209,000 more than in 2019.[1]

Research for the *2022 State of the Phish* shows just how prevalent and effective phishing attacks are. It found that in 2021:



of organisations faced bulk phishing attacks[2]

1 in 5

●○○○○

users opened an attachment in phishing simulations

1 in 10

◐○○○○

users clicked on a link in phishing simulations

Real-world example: Ukrainian government electric grid shutdown

In December 2015, Ukraine's power grid was disrupted, knocking out service up to six hours for about 225,000 people in the Eastern European country. It was the first publicly acknowledged cyber attack that resulted in power outages.[3]

The threat actors behind the attack spent months strategising and gathering intelligence. Among the techniques they used to carry out their plan was spear phishing. In this case, the targets were IT staff and system administrators at three Ukrainian energy distribution companies (or oblenergos).[4]

[1] FBI IC3. "Internet Crime Report 2021." March 2022. Available at: https://www.ic3.gov/Home/AnnualReports.

[2] Proofpoint defines bulk phishing as indiscriminate, "commodity" attacks in with the same email is sent to many people within an organisation.

[3] SANS Industrial Control Systems (ICS) and Electricity Information Sharing and Analysis Center (E-ISAC). "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case." March 18, 2016.

[4] ICS and E-ISAC.

How it worked

To compromise these users, the attackers sent a malicious Microsoft Word attachment in an email that appeared to be from a trusted source. When opened, the document displayed a pop-up that asked the user to enable macros. If the user complied, malware called BlackEnergy3 then infected the machine, providing a backdoor for the attackers.[5]

These spear-phishing attacks gave the criminal actors access to the energy company's network. From there, the adversaries then spent months steadily winding their way to the companies' supervisory control and data acquisition (SCADA) industrial-control networks to set up their big attack. They used various methods, including gaining access to Microsoft Windows Domain Controllers to harvest even more user account credentials.[6]

The outcome

The power outage was brief. Still, it took months for the control centres in the affected oblenergos to become fully operational again. And as one report about the attack noted, the incident "set an ominous precedent for the safety and security of power grids everywhere."[7]

Phishing: potential consequences

Account takeover

Financial loss

Data loss

Reputational damage

How user awareness could have helped

Like most cyber attacks, the 2015 grid shutdown started with a phishing email. After tricking an employee into opening an infected attachment, threat actors spent months gathering intel and burrowing more deeply into the environment.

Security awareness training might have helped stop the attack before it began. The employee would have known not to open or interact with the attachment, denying the attacker entry.

[5] Kim Zetter *(Wired)*. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." March 3, 2016.
[6] Ibid.
[7] Ibid.

SECTION 2

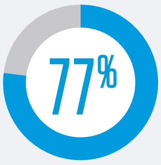
Business Email Compromise (BEC)

Business email compromise (BEC) attacks target organisations of all sizes across every industry.

BEC attackers pose as a person or entity that the recipient is likely to trust, such as company's chief executive or a vendor. The attacker then directs the recipient to make wire transfers, divert payroll, change banking details for future payments or take other actions. By the time the victim discovers an error, it's often too late to recoup the losses.

Trends

BEC campaigns can deliver big returns. The FBI's *2021 Internet Crime Report* says BEC attacks resulted in an adjusted loss of $2.4 billion last year in the United States alone.[8] Given the potential payoff, it's no surprise that the *2022 State of the Phish* found that 77% of organisations around the world faced BEC attacks in 2021.



of organisations around the world faced BEC attacks in 2021

BEC is often highly advanced, well-funded and backed by careful planning and research.[9] Many attackers focus their efforts on supplier invoicing fraud because of the sizable business-to-business transactions they can hijack. False invoice schemes are a common tactic. In these attacks, the scammer pretends to be a supplier and diverts payments that should go to real vendors.

Real-world example: Ubiquiti loses $46.7 million to vendor fraud

Another well-worn yet effective BEC strategy is CEO fraud, where attackers pose as the CEO or another top executive. Typically, they'll email someone who works in the finance department to request a funds transfer—with the money often going to an international account that the attacker controls.

Ubiquiti Inc. was targeted with this type of BEC scam. Cyber criminals managed to siphon off $46.7 million from the technology firm before anyone realised there was a problem. Users who have the authority to transfer funds may not think to question financial-related requests from top executives—even if those requests seem unusual.

How it worked

Just a few weeks into the job in mid-May 2015, Ubiquiti's new chief financial officer (CFO) received emails he believed were from the company's CEO and a London-based attorney. The scammer posing as the CEO explained that the company was pursuing an acquisition. According to the email, the CFO needed to keep this under wraps, and several wire transfers were needed to move the deal forward. The impostor followed up by sending fake email instructions and banking details and authorising the payments.[10]

[8] FBI IC3.

[9] Proofpoint. "You've Got Email Fraud! A Roundup of the Biggest, Boldest and Most Brazen Business Email Compromise Attacks." April 2022.

[10] Nathan Vardi *(Forbes)*. "How a Tech Billionaire's Company Misplaced $46.7 Million and Didn't Know It." February 2016.

The outcome

Over the course of 17 days, the CFO made 14 wire transfers—totaling $46.7 million—to accounts in China, Hungary, Russia and Poland. Then, in early June, the company's real CEO was contacted by an FBI agent. Agents informed him that a large sum of money may have been stolen from the bank account of Ubiquiti's Hong Kong unit.[11] Until then, the CEO didn't even know about the wire transfers.

In August 2015, Ubiquiti disclosed in a quarterly financial report filed with the U.S. Securities and Exchange Commission that it had discovered fraud in June, describing the incident as "employee impersonation and fraudulent requests from an outside entity."

Ubiquiti was able to recoup only some of its losses and the company suffered reputational damage. Its CFO resigned just before the company publicly disclosed the BEC incident. An internal probe concluded that its internal control over financial reporting was ineffective, and the company moved to shore up its controls.[12]

BEC: potential consequences

Direct financial loss

Data loss

How user awareness could have helped

Vendor fraud and other forms of BEC are inherently people-focused attacks. They succeed only when recipients think they're dealing with someone they can trust. With effective security awareness education, the CFO might have known to look for tell-tale signs that the emails were from an impostor and not the CEO and company lawyers.

Combined with the sound fiscal controls, user education can train your people to instinctively spot lookalike or unrelated domains, unsafe URLs and social engineering techniques that might snare users who are less aware.

[11] Ibid.

[12] KrebsonSecurity. "Tech Firm Ubiquiti Suffers $46M Cyberheist." August 2015.

SECTION 3

Ransomware

At its core, ransomware is a tool that enables extortion. It's malware that locks away data and computer systems until the victim pays to regain access.

Usually, the attacker requires payment in cryptocurrency such as Bitcoin because the money is fast and hard to trace. The demand often comes with a deadline: if victims don't pay on time, they'll either lose their data for good or need to pay a higher ransom to get it back. To pressure victims even further, attackers often threaten to publish the data. In some cases, victims may pay and still lose their data.

Encrypters and screen lockers are the main types of malware used in ransomware attacks. The first encrypts data on a system, making the content useless without a decryption key. Screen lockers use a “lock” screen to block users’ access to the compromised system.

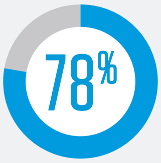
Ransomware attacks have existed for decades. But they’ve been grabbing a lot of media attention in recent years due to the major disruption they cause, the massive payments they demand and critical infrastructure they target, especially in the healthcare and energy sectors.

At the same time, they have evolved. Ransomware operators often buy access from independent cyber criminal groups who infiltrate major targets and then sell access to others for a slice of the ill-gotten gains. Threat groups already distributing banking malware or other Trojans may also become part of a ransomware affiliate network. The result is a robust and lucrative criminal ecosystem in which people and organisations have specialised to optimise profits for everyone—except, of course, the victims.

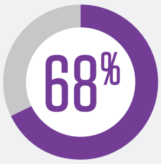
Trends

Ransomware attacks are also on the rise. Verizon’s *2022 Data Breach Investigations Report*” notes that ransomware breaches increased 13% from 2020 to 2021—an increase as big as the past five years combined.[13]

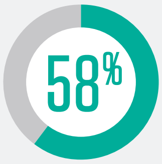
Here are a few ransomware findings from the *2022 State of the Phish* report:



of organisations saw email-based ransomware attacks in 2021



of organisations were infected by ransomware



of infected organisations paid a ransom

[13] Verizon. “Data Breach Investigations Report.” May 2022.

Real-world example: Back-to-back ransomware attacks create extended chaos for Costa Rican government

A severe ransomware attack hit the Costa Rican government in April 2022, targeting nearly 30 institutions. These included Costa Rica's Ministry of Finance, the Costa Rican Social Security Fund and even the National Meteorological Institute. The Conti ransomware group claimed responsibility for the campaign and demanded a ransom of US$10 million in exchange for not releasing sensitive information it had siphoned from the Ministry of Finance's servers before the attack.[14]

When the government refused to pay, Conti increased the ransom demand to $20 million; soon after, the group started uploading stolen files to their website. In a failed, last-ditch effort to get a payout, Conti group reduced the ransom demand to $15 million.[15] Also, in an odd and disturbing twist to this story, the attackers threatened to overthrow the government.[16]

In late May, as the Costa Rican government was still trying to recover from Conti group's attack, the national health service (CCSS) suffered a ransomware attack launched by a group known as Hive. The agency became aware of the attack when its printers began churning out copies of Hive's ransom note, which didn't include a ransom amount.[17] That demand would come later, when Hive asked the CCSS for a payment of $5 million in bitcoin in exchange for not leaking sensitive information.[18]

[14] Carly Page *(TechCrunch)*. "Fears Grow for Smaller Nations After Ransomware Attack on Costa Rica Escalates." May 20, 2022.

[15] Carla Rosch *(Rest of World)*. "A Massive Cyberattack in Costa Rica Leaves Citizens Hurting." June 1, 2022.

[16] Matt Burgess *(Wired)*. "Conti's Attack Against Costa Rica Sparks a New Ransomware Era." June 12, 2022.

[17] KrebsonSecurity. "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions." May 31, 2022.

[18] Alonso Martinez *(Delfino)*. "Cybercriminals Request $5 million in Bitcoins from the CCSS." June 2, 2022.

How it worked

According to threat researchers, a member of the Conti group known as "MemberX" used compromised credentials to gain access over a VPN connection to a system belonging to Costa Rica's Ministry of Finance.[19] Within 24 hours of the first Conti attack, the attackers had encrypted files within the finance ministry and sidelined two critical systems: the digital tax service and the IT system for customs control.[20]

Some speculate that Conti may have had insider help. In fact, one message the group released on the dark web after the attack stated that "insiders in [the Costa Rican] government" provided help—a threat actor it called "UNC1756."[21]

As for Hive, the group relies on a ransomware-as-a-service (RaaS) model for its attacks. The group and its affiliates send phishing emails with malicious attachments, seek out VPN credentials, and use vulnerable remote desktop protocol (RDP) servers to move laterally within the now-compromised network. According to an FBI advisory about Hive, the group will typically exfiltrate data and encrypt files on the network. Then it leaves a ransom note in each affected directory within a victim's system. The note provides instructions on how to purchase the decryption software and threatens to leak exfiltrated victim data on the Tor site, "HiveLeaks."[22]

Some cybersecurity experts believe that the same cyber criminals had a hand in both springtime ransomware attacks. They suggest that Hive used its campaign to help Conti rebrand and evade international sanctions banning extortion payouts to cyber criminals that operate in countries known to tolerate (if not support) this activity.[23] Hive has claimed on its website that it isn't affiliated with Conti.[24]

The outcome

In the wake of the first ransomware attack in mid-April, the Costa Rican economy was losing about $30 million per day. The government was forced to shut down many critical systems during the chaotic remediation phase. The Costa Rican Chamber of Foreign Commerce alone estimated losses of over $125 million in just the first two days after the attack.[25]

[19] Ionut Ilascu *(BleepingComputer)*. "How Conti Ransomware Hacked and Encrypted the Costa Rican Government." July 21, 2022.

[20] Matt Burgess *(Wired)*. "Conti's Attack Against Costa Rica Sparks a New Ransomware Era." June 12, 2022.

[21] Claudia Glover *(Tech Monitor)*. "'We will overthrow the government' – Does Conti have help inside Costa Rica?" May 17, 2022.

[22] FBI FLASH report. "Indicators of Compromise Associated with Hive Ransomware." August 25, 2021.

[23] KrebsonSecurity. "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions." May 31, 2022.

[24] Ibid.

[25] Carla Rosch *(Rest of World)*. "A Massive Cyberattack in Costa Rica Leaves Citizens Hurting." June 1, 2022.

The government also had to take down webpages for the targeted agencies. It enlisted technical help from other governments, including the U.S., and technology companies such as Microsoft. The U.S. even offered up to $5 million for information that could lead to the arrest or conviction of anyone conspiring in a Conti ransomware attack.[26]

In early May, the new president of Costa Rica, Rodrigo Chaves Robles, declared a national state of cybersecurity emergency, calling the Conti attack an act of terrorism. Within a few weeks, Hive launched its attack.

The Costa Rican struggled for weeks to recover. By mid-June, some agencies could finally resume operations.

Ransomware: potential consequences

Business disruption

Financial loss
(due to paying the ransom and actions related to remediating the attack)

Data loss
(if attackers follow up on threats to leak data if the ransom isn't paid)

How user awareness could have helped

Some reports suggest the ransomware attack against Costa Rica may have been helped along by malicious insiders. But many ransomware infections are the byproduct of earlier email-borne compromises. Attackers use techniques such as phishing to steal user credentials that can provide them access to critical systems.

Training users to spot and report suspicious email, especially in conjunction with automated closed-loop analysis, can dramatically reduce the risk from ransomware and other forms of malware.

Users should know to instinctively distrust file attachments and URLs—especially in emails that lean into natural human instincts such as personal gain, curiosity, fear, outrage and even helpfulness. And they should know the signs that the sender may not be who they purport to be.

[26] Elizabeth Montalbano *(Threatpost).* "Conti Ransomware Attack Spurs State of Emergency in Costa Rica." May 10, 2022.

SECTION 4

Cloud Attacks and Account Takeover

Attackers go where users go. Increasingly, that's to the cloud. The COVID-19 pandemic has accelerated a shift to the cloud and, as a result, cloud attacks are growing more common. As our *The Human Factor Report 2022* explains, cloud account compromise has become a substantial and permanent feature of the cyber threat landscape—just like phishing and malware.

Cloud account compromise is the act of maliciously gaining control over a legitimate user's cloud-based email or collaboration service account. These cloud account takeovers can lead to attackers gaining wide-ranging access to a user's data, contacts, calendar entries, email and other system tools. And by abusing single sign-on authentication, bad actors are free to roam across many different systems in the environment and cause widespread damage.

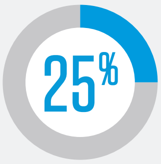
Tools that attackers often use to compromise cloud accounts and enable a takeover include:

- Brute-force attacks that automate credential-guessing
- Phishing attacks, including OAuth token phishing
- Credential recycling or stuffing, using already-stolen username and password pairs
- Malware, such as keyloggers and credential stealers

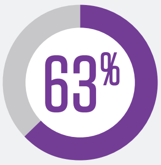
Persistence appears to be another key ingredient in cloud account compromise.

Trends

Data in *The Human Factor Report 2022* shows that over 90% of monitored cloud tenants were targeted by attackers every month. Nearly one-quarter (25%) were successfully attacked—with nearly two-thirds of tenants (63%) compromised during the course of the year.[27]



of monitored cloud tenant attacks were successful



of cloud accounts were compromised in 2021

Cloud account takeovers are often hard to detect, challenging to resolve and damaging to your bottom line. A recent study found that the average yearly financial loss for businesses due to compromised cloud accounts is $6.2 million. Organisations also experience 138 hours of application downtime, on average, due to this activity.[28]

Malicious cloud applications

Shadow IT contributes to the malicious cloud apps issue. Third-party cloud applications are apps that integrate with a cloud service but aren't provided by the cloud vendor. Third-party apps use OAuth, an authorisation protocol that allows the apps to obtain limited access to a cloud service. OAuth also enables third-party apps to use a user's account information or data without exposing credentials.[29]

This all sounds very convenient and secure. But unfortunately, third-party apps are easily exploited. When users install them, they often click "accept" without closely reviewing the scope of permissions. Once attackers gain OAuth access, they can compromise and hijack cloud accounts. Worse, they have persistent access to the users' accounts and data until the OAuth token is explicitly revoked.

[27] Proofpoint. "The Human Factor 2022." May 2022.

[28] Ponemon Institute. "2021 Ponemon Report: The Cost of Cloud Compromise and Shadow IT." April 2021.

[29] Proofpoint. "What Every Security Professional Should Know About Third-Party OAuth Apps." May 2022.

Malicious files stored in the cloud

Once an attacker takes over a cloud account, they can upload malicious files to lay the groundwork for other mischief, like data theft or wire fraud. For example, in a Microsoft SharePoint phishing scheme, an attacker uploads a malicious file to a compromised cloud account. The file's sharing permissions are changed to "Public" so that the new anonymous link can be shared with anyone. The attacker then emails or shares the link with the compromised user's contacts or other targets. Once those recipients open the file and click on the malicious link, they're phished.[30]

Our threat researchers recently uncovered a brand new twist on cloud attacks: attackers now target data in the cloud and launch ransomware-style attacks using cloud infrastructure. And they're compromising popular enterprise cloud apps in the process, including SharePoint Online and OneDrive within the Microsoft 365 suite.[31]

Despite the very real danger that attacker-compromised files in the cloud can pose, the *2022 State of the Phish* report found that only 37% of users are aware that files stored in the cloud can be malicious.

Real-world example: OiVaVoii campaign

The cloud makes collaboration and data-sharing easier. It's also a complex threat environment that's growing quickly amid digital transformation and remote and hybrid work.

A recent campaign that targeted high-value users, including the C-suite, shows why users at all rungs of the corporate ladder must be cautious about granting permissions to cloud apps. That's true even if those apps seem benign and appear to be from legitimate senders.

[30] Itir Clarke, Eilon Bendet and Doyle Groves. *(Proofpoint).* "Why OneDrive and SharePoint Attacks Are Successful and How to Fight Back." October 2020.

[31] Or Safran, David Krispin, Assaf Friedman and Saikrishna Chavali *(Proofpoint).* "Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive." June 2022.

How it worked

In January 2022, our researchers first observed a malicious hybrid cloud campaign, OiVaVoii, and uncovered five malicious OAuth applications linked to the campaign.[32]

At least three of the malicious third-party apps were created by two different "verified publishers." These publishers were likely compromised administrative user accounts within legitimate Microsoft 365 tenants. Of the remaining two apps, at least one was created by a non-verified publisher. This suggests that the attackers were using a third hijacked cloud environment or dedicated malicious Microsoft 365 tenant.

The outcome

Once the attackers created the apps, they sent authorisation requests via email to numerous targeted users, including high-level executives. Many of those users authorised the apps. That simple action enabled the attackers to generate OAuth tokens on behalf of the targeted user and complete the account takeover. All the apps associated with the OiVaVoii campaign requested similar permissions from users, primarily for mailbox access (read and write). Once users accepted the requests, the attackers were free to send malicious email messages internally and externally, steal valuable information and more.

Cloud attacks: potential consequences

Account takeovers

Data loss
(due to malware entering the environment or direct siphoning of data by malicious apps)

Business disruption
(from ransomware and other malware entering the environment)

How user awareness could have helped

Like most email attacks, cloud-based attacks rely on human interaction—unknowingly giving up their credentials, installing malicious apps and clicking on URLs to trusted file-sharing sites used to host malicious files.

Teaching your people to use cloud services safely—and be wary of authorising unknown apps—should be a critical part of your security awareness programme.

[32] Eilon Bendet, Assaf Friedman and David Krispin *(Proofpoint)*. "OiVaVoii – An Active Malicious Hybrid Cloud Threats Campaign." January 2022.

Why multifactor authentication is no silver bullet

Many security-aware organisations teach users to employ multifactor authentication (MFA) as a tool to help safeguard users' accounts—and rightly so. MFA is another layer of security that helps safeguard accounts when an attacker tries to log in with stolen credentials. When logging in, it requires the user to enter not just their username and password but also a code from their phone, fob or physical security key. MFA greatly reduces the chances that attackers can compromise accounts through stolen credentials alone and should be part of every security programme.

But it's not failsafe. Easy-to-use phishing kits are making it easy for attackers to sidestep these protections. Microsoft says that threat actors bypassed MFA in attacks that targeted more than 10,000 organisations from September 2021 onward. Once attackers gained access, they used compromised accounts to launch BEC attacks.[33]

These attacks typically start with a phishing email, so it's critical to teach users how to recognise and report suspicious messages. In the Microsoft attack, phishing emails included an HTML attachment. When opened, the file redirected users to a proxy server that intercepted traffic between users and the login screen.

Users should also know to never open file attachments from unknown senders. That's especially true for file types not normally sent by email.

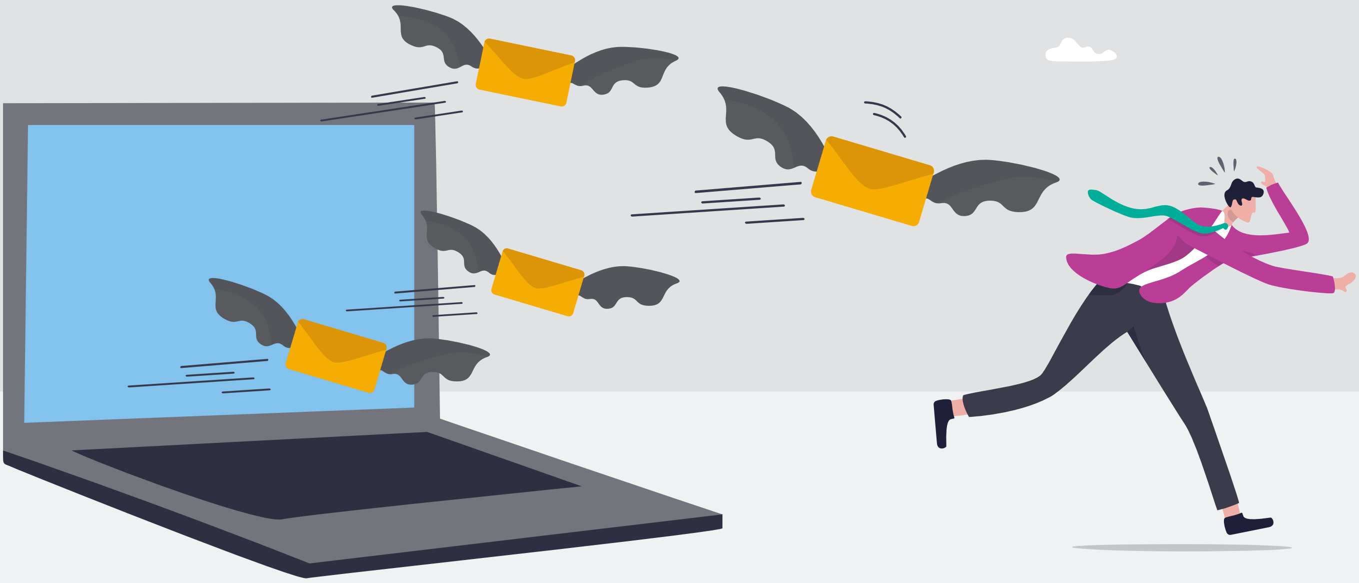
[33] Microsoft. "From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud." July 2022.

SECTION 5

Web-Based Email Attacks

The rise of remote work is providing cyber criminals even more opportunity to gain access to corporate systems. Most employees use a virtual private network (VPN) to access their company's network when working off-site. And they're also using their own devices to connect to corporate resources. These are the same devices they use to access their personal, web-based email accounts. Conversely, many workers use work-issued devices to access their personal accounts.

If attackers compromise a user's non-work-related accounts, they can then find credentials to enterprise applications, data and systems. They can also take advantage of the fact that many employees use their personal email accounts or mobile numbers for two-factor authentication or password resets. With that information in hand, attackers don't have to do much more to gain access to corporate networks.

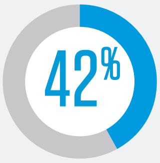


Trends

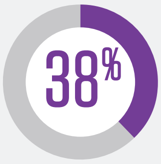
Data compiled for the *2022 State of the Phish* report suggests many users are at risk for web-based email attacks that could harm their employers.

Also, it seems many users might assume their web-based email providers will protect them from these attacks.

Our research found that:



of users access personal email on work-issued devices



of users know their personal email provider can't block all dangerous email

Real-world example: LAPSUS$

Sometimes, what cyber attackers care about just as much or even more than making money is creating disruption and getting a lot of attention for it. That describes the data-stealing and extortion gang LAPSUS$, which emerged in late 2021. The group may still be active despite several of its members—all between the ages of 16 and 21—being arrested by U.K. police in March.[34]

How it worked

In a few short months, The LAPSUS$ group tried to extort Brazil's Ministry of Health and posted screenshots of internal tools tied to NVIDIA, Samsung and Vodafone.[35] It drew notice for its unconventional approach to extortion. It stole sensitive data and then threatened to publish it online unless the victim paid up. Essentially, it was a ransomware attack without the ransomware.

The outcome

The group was so bold that they would poll users on the Telegram app to vote for which victim's data it should publish online next.[36] To get access to the corporate networks it wanted to compromise, the LAPSUS$ group would often target employees' personal email accounts to look for credentials and systems for enabling remote access.[37]

[34] Scott Ikeda *(CPO Magazine)*. "Suspected Lapsus$ Hackers Arrested; London Group Between the Ages of 16 and 21." March 2022.

[35] Krebs on Security. "A Closer Look at the LAPSUS$ Data Extortion Group." March 2022.

[36] Lily May Newman *(Wired)*. "The Lapsus$ Hacking Group Is Off to a Chaotic Start." March 2022.

[37] Microsoft. "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction." March 2022.

Microsoft Security teams refers to the LAPSUS$ gang as “DEV-0537.”

“Unlike most activity groups that stay under the radar, DEV-0537 doesn’t seem to cover its tracks,” the software giant says. “They go so far as announcing their attacks on social media or advertising their intent to buy credentials from employees of organisations in their sights.”[38]

The group’s “advertising” included Telegram messages, in which LAPSUS$ would try to recruit employees and other insiders at telecoms, large software and gaming corporations, call centre operators and server hosts. Their goal: bribe employees to get VPN credentials or some other form of remote access. LAPSUS$ also offered payment to cooperating insiders. One ad described an opportunity to earn $20,000 or more per week.[39]

Microsoft Security has also reported that LAPSUS$ gained initial access to victims by other means. One of these means was purchasing credentials and sessions tokens from criminal underground forums. Another method was searching public code repositories for exposed credentials.

Web-based email attacks: potential consequences

Data loss

Business disruption

Financial loss

Reputational damage

How user awareness could have helped

The LAPSUS$ group’s activity involved various tactics, including:

- Compromising web-based email and remote access methods
- Recruiting of company insiders, suppliers or business partners
- Stealing sensitive data and intellectual property
- Ransom demands

Showing users how to protect their credentials, use personal email safely and report ransom demands would have gone a long way towards avoiding falling victim.

[38] Ibid.

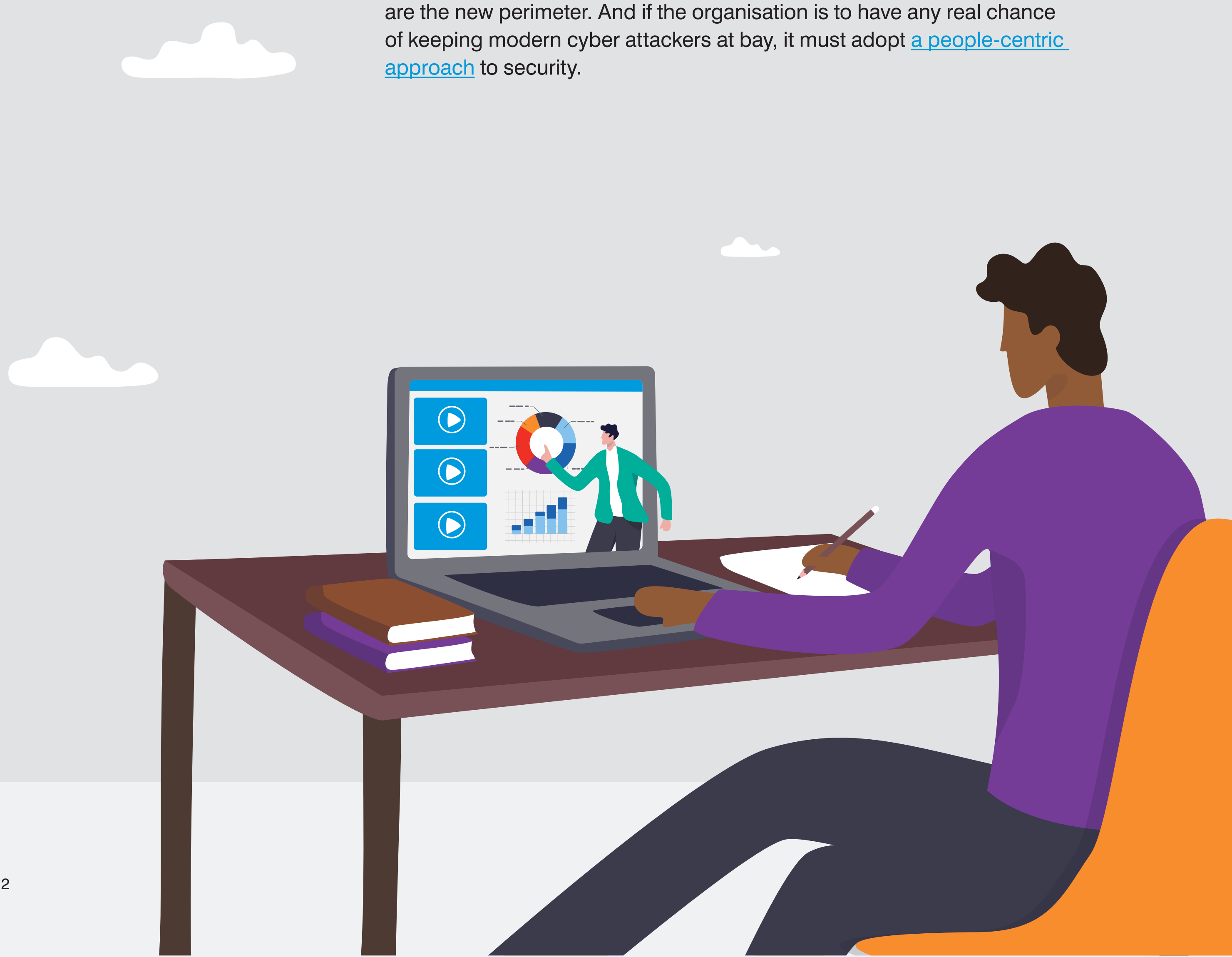
[39] KrebsonSecurity. “A Closer Look at the LAPSUS$ Data Extortion Group.” March 2022.

SECTION 6

Conclusions and Recommendations

The challenge is determining the best way to educate your users about the always-evolving threat landscape—and keep them informed. Ultimately, your aim is to motivate them to be as vigilant about cyber threats as your security teams. Then they can become proactive defenders.

For security awareness education to work, your users will need to understand the “So what?” Why should they care about cyber threats? Why is defending the organisation partly their responsibility? The short answer is that they are the new perimeter. And if the organisation is to have any real chance of keeping modern cyber attackers at bay, it must adopt a people-centric approach to security.



The five types of cyber threats and attack examples discussed in this e-book share this in common: they target people. The attackers enlist users' help, willing or not, to advance their campaigns and achieve their goals.

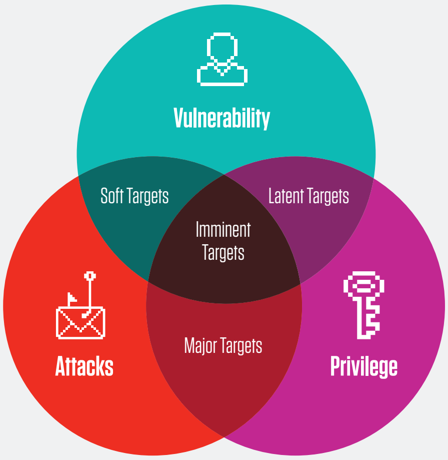
These threats and incidents help demonstrate that people are the most critical factor in today's threat landscape. That's why security awareness training for users should be a core part of your cybersecurity strategy.

Prioritise what's important

Everyone who can influence your organisation's cybersecurity posture should be trained in cybersecurity best practices. But you should be deliberate and strategic about how you assess and train your people.

Also, prioritise topics you know are relevant to your industry and organisation—and the people who work within them. Consider using the real-world examples showcased in this e-book to help connect with user audiences most likely to relate to these stories. That's because they're sure to face similar attacks due to the nature of their job, title, where and how they work, and other factors.

Use threat intelligence to your advantage



Threat intelligence can also help you decide when to provide specific training to specific people. To use insights about known and emerging threats to your advantage, it's also critical to identify the following users:

Highly vulnerable users—as determined by their behaviour, their tendency to click on simulated phishing emails and their participation in training.

Highly attacked users—those who face a high volume of attacks, especially sophisticated attacks, narrowly targeted attacks or any combination thereof.

Highly privileged users—those who have access to valuable data, systems and other critical resources the organisation must safeguard.

In short, a successful people-centric security approach requires understanding the people and departments within your organisation that are being attacked and targeted at any given time. It also means knowing what methods attackers are using to attempt to compromise your users and environment.

Continually evaluate key security awareness metrics to gauge success

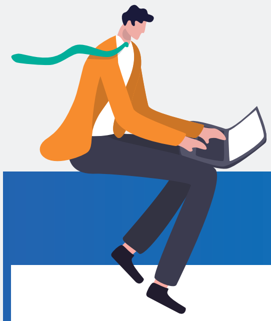
Avoid framing your view of training success on a single measurement—like phishing test failure rates. To measure “success,” you should include multiple components and also take organisational factors into account.

Consider using the following metrics:

- Phishing simulation failures
- Phishing simulation reporting
- Knowledge assessments
- Reported email accuracy
- Training participation

As a final tip, remember that security awareness training needs to evolve to keep pace with the ever-changing threat landscape. Ensure the guidance you’re providing is relevant to your users because your organisation is always changing, too. The metrics outlined above can help you continuously gauge the effectiveness of your programmes and adjust as needed.

For more details on these strategies for improving your security awareness training programmes, download the *2022 State of the Phish* report from Proofpoint.

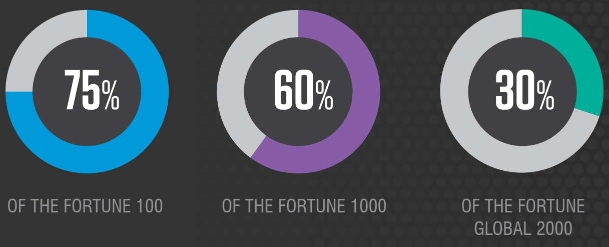


Why Proofpoint

Every day, we analyse more than:

2.6B EMAILS	49B URLS	1.9B ATTACHMENTS
1.7B MOBILE MESSAGES	430M WEB DOMAINS	143,000 SOCIAL MEDIA ACCOUNTS

We are trusted by more than:



8,000
ENTERPRISES

200,000
SMALL BUSINESSES

LEARN MORE

For more information, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations of all sizes, including 75 percent of the Fortune 100, 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.