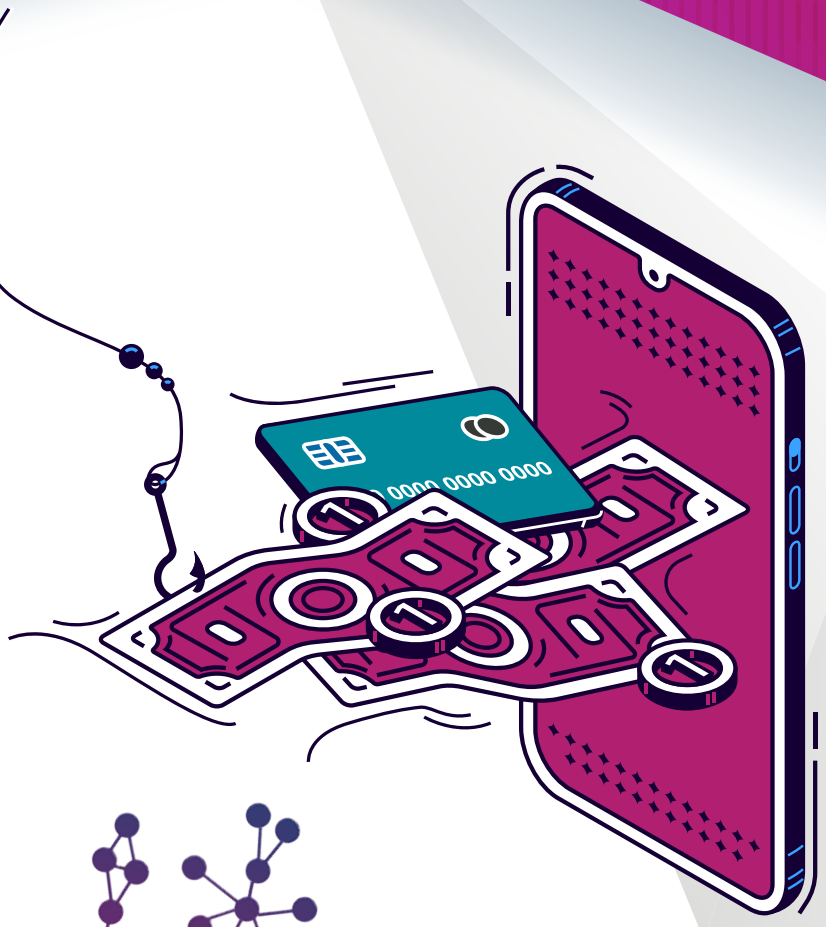
GRAPHUS
A Kaseya COMPANY

PHISHING 101

Protecting your business from cybercrime starts by protecting it from phishing.



PHISHING IS THE STAR OF THE CYBERCRIME WORLD

Protecting your business from cybercrime starts by protecting it from phishing. From business email compromise to ransomware, all of today's most damaging cyberattacks start with phishing. In fact, some of the most famous cyberattacks in history started with a phishing email. That's why 65% of active cybercriminal gangs use phishing as their primary method of attack.

This perennial cybercriminal favorite threatens every organization no matter the size and wears many devious disguises. Go behind the scenes of phishing to see how it works and discover how to beat it.

That's why 65% of active cybercriminal gangs use phishing as their primary method of attack.

LEARN THE LANGUAGE

It can feel like you need to learn a whole new language to learn about cybersecurity. Before we look at strategies to combat phishing, we must first make sense of the chatter.

A whole new language

Account Takeover (ATO): A form of identity theft and fraud, the goal of an ATO attack is for a malicious third party to capture and exploit a user's account credentials, enabling the attacker to pose as the victim for other operations.

Angler Phishing: Phishing through social media that includes direct messages and phony alert emails from social media sites.

Brand Impersonation: Pretending to send messages from a well-known brand to masquerade as a trusted source.

Business Email Compromise (BEC): Using legitimate email accounts from a business partner to fraudulently obtain money or data.

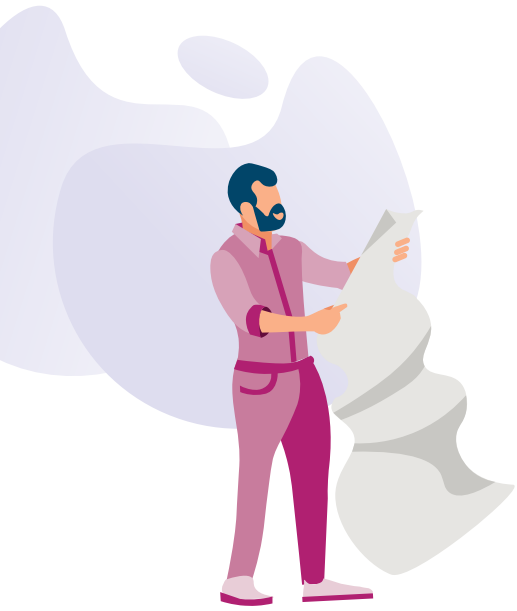
Credential Theft: Tricking the victim into providing their credentials to bad actors, sometimes using a website or link.

Filter: Shields used by software to funnel traffic, like spam email, into another location.

Lure: Also called bait or a hook, the lure is the email or message that "phishermen" use to attract the target's attention.

Malware Attack: A piece of malicious code or software that infects systems to facilitate cybercrime like data encryption or theft. All ransomware is by nature malware, but there are other types of malware, like key loggers and payment skimmers, that can be delivered via phishing.

Phishing Attack: A cyberattack in which a cybercriminal sends a victim a message that is designed to lure them into taking an action that facilitates another kind of cyberattack against the victim, like getting someone to open an attachment that contains ransomware. Phishing can also defraud the victim out of valuable information like passwords.



Phishing Resistance: This is the amount of savvy that employees show when faced with phishing – a skillset that enables them to spot and stop dangerous messages.

Payload: The "bomb" that a phishing message carries that is typically some manner of malware or ransomware.
Quarantine: A separate system location where dangerous messages are sent for review for a preset period of time, in order to prevent them from reaching most employees.

Ransomware: A subtype of malware, ransomware encrypts a victim's data and systems, enabling cybercriminals to demand a ransom for the decryption key. Ransomware can also be used to steal data, shut down production lines, and take infrastructure offline. It is the preferred weapon of nation-state cybercriminals.

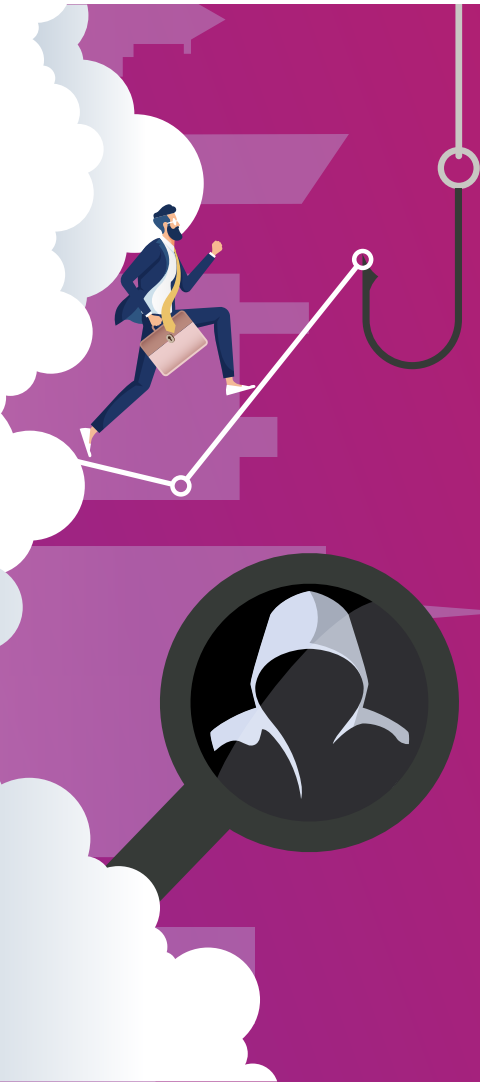
Spear-Phishing: Learning details about the target and then crafting an email that will entice them to interact with it. This is the most common form of phishing, often utilizing data about the victim gathered from the dark web. It's also the primary delivery system for malware and ransomware.

Spoofing: Attacks that take a legitimate message, cloning it, and then using it to facilitate a phishing attack.

Whaling/CEO Fraud: A highly targeted, sophisticated attack aimed at a CEO or another senior executive in order to persuade them to perform an action, such as a wire transfer of funds.

SOCIAL ENGINEERING PRIMER

At the core of a phishing attack, the cybercriminal's goal is to gain the trust of their victims to trick them into taking an action that will facilitate the bad actor's desired result. Social engineering is the X-factor that makes phishing so effective. Savvy cybercriminals will put time and effort into social engineering in order to perpetrate believable frauds that lure targets into a false sense of security. **Examples include:**



- Preying on the target's emotions by stoking fear or anxiety
- Exploiting natural disasters or emergencies like the COVID-19 global pandemic
- Evoking a false sense of security through nostalgia or brand reputation
- Creating boring, routine emails that don't raise suspicion, like a password reset request
- Simulating messages employees deal with every day, like system notifications Mimicking internally facing corporate emails that staffers will feel compelled to read
- Raising excitement or greed by promising the target a reward for following directions
- Imitating a business partner to persuade the victim to disclose proprietary information
- Posing as tech support to gain access to passwords
- Sending believable fake invoices and demanding payment from the target

PHISHING ATTACKS:
ESSENTIAL STATISTICS

In a world full of buzz about cybersecurity, one indisputable fact is clear: since early 2020, phishing has been the biggest threat to business cybersecurity worldwide. These essential facts about phishing threats will help you focus on the real danger today's phishing attacks pose to your business.

1. **90%** of incidents that end in a data breach start with a phishing email.
2. **80%** of firms have seen an increase in cyberattacks since March 2020
3. **75%** of organizations around the world experienced a phishing attack in 2020.
4. **94%** of ransomware and other nasty malware arrives at businesses via email.
5. **65%** of organizations faced BEC attacks.
6. **74%** of organizations in the United States experienced a successful phishing attack.
7. **40%** of remote workers have made email-handling errors that caused cybersecurity incidents.
8. **More than 80%** of reported security incidents are phishing related.
9. Phishing risk rose by **more than 600% in 2020**.
10. A new cyberattack like phishing is launched **every 39 seconds**.

But that's not all. Google has registered **2,145,013** phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months).

Approximately 1.5 million new phishing sites are created every month.

In 2020, BEC costs increased rapidly from $54,000 in Q1 2020 to $80,183 in Q2. The average ransomware payment in the **third quarter of 2020 was $233,817**, up 31% from the second quarter of 2019.

A single spear-phishing attack results in an average loss of $1.6 million.

WHO FALLS FOR PHISHING?

While every business is at risk of a phishing attack every day, some industries are more vulnerable than others. A 2020 user behavior study explored which sectors have employees most likely to interact with a phishing email.

Top 5 Sectors in Which Employees Interact with Phishing Messages

1. Consulting
2. Apparel and accessories
3. Education
4. Technology
5. Conglomerates/multinationals

Top 5 Sectors in Which Phishing Leads to Credential Compromise

1. Apparel and accessories
2. Consulting
3. Securities and commodity exchanges
4. Education
5. Conglomerates/multinationals

An estimated **97% of employees** in a wide array of industries are unable to recognize a sophisticated phishing email. So, what are they most likely to do when they receive a phishing message?

1 in 3
employees are likely to click the links in phishing emails.

60%
of employees opened emails they weren't fully confident were safe.

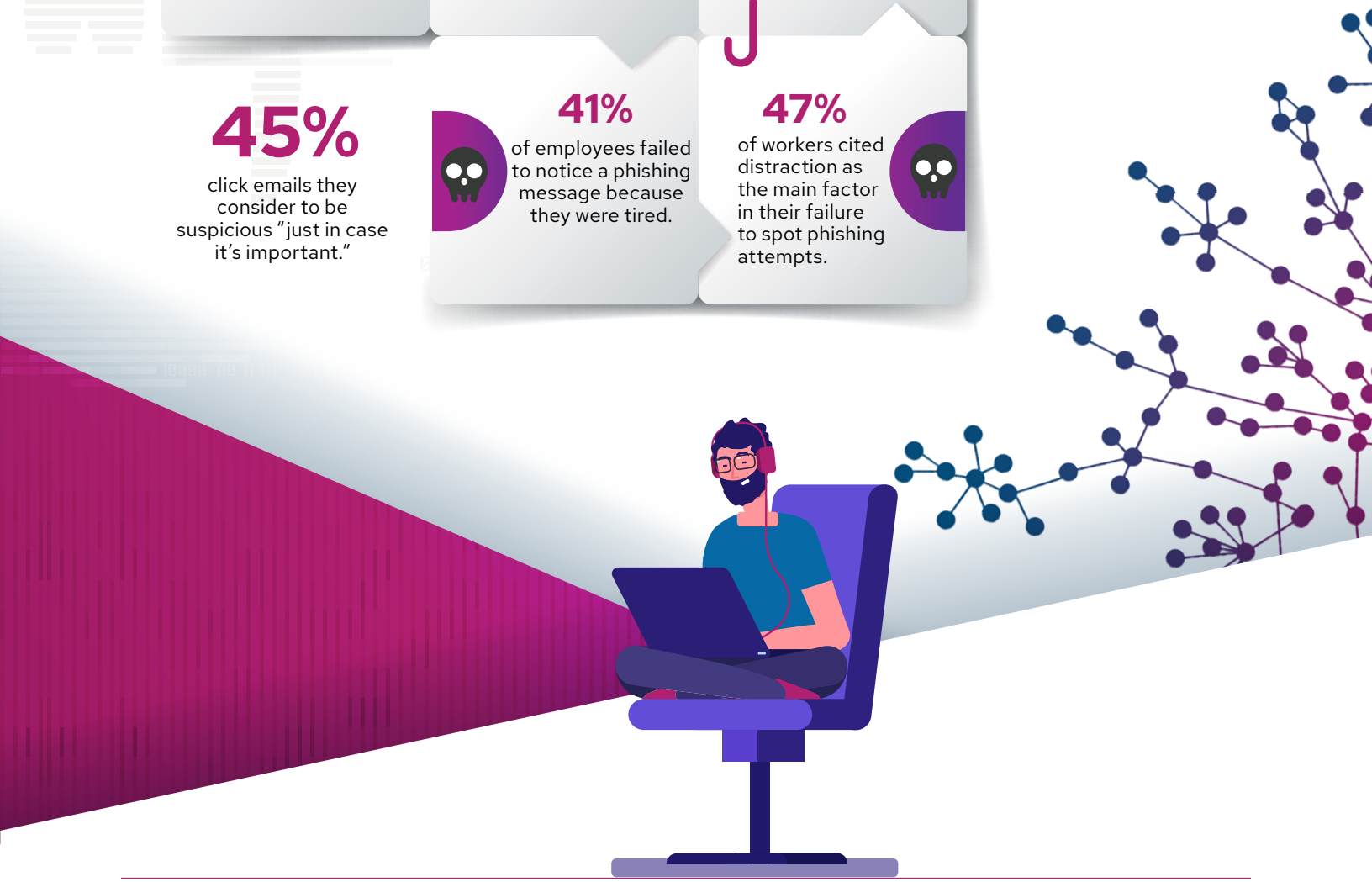
1 in 8
employees are likely to share information requested in a phishing email.

45%
of employees never report suspicious messages to IT for review.

45%
click emails they consider to be suspicious "just in case it's important."

41%
of employees failed to notice a phishing message because they were tired.

47%
of workers cited distraction as the main factor in their failure to spot phishing attempts.



LEARN FROM THESE
CYBERSECURITY DISASTERS

When you look at the most damaging cyberattacks in history, you'll see that the majority of them have one thing in common – their point of origin was a phishing email. Take a look at these massive cybersecurity disasters in 2020 that were launched with just one fatal click.

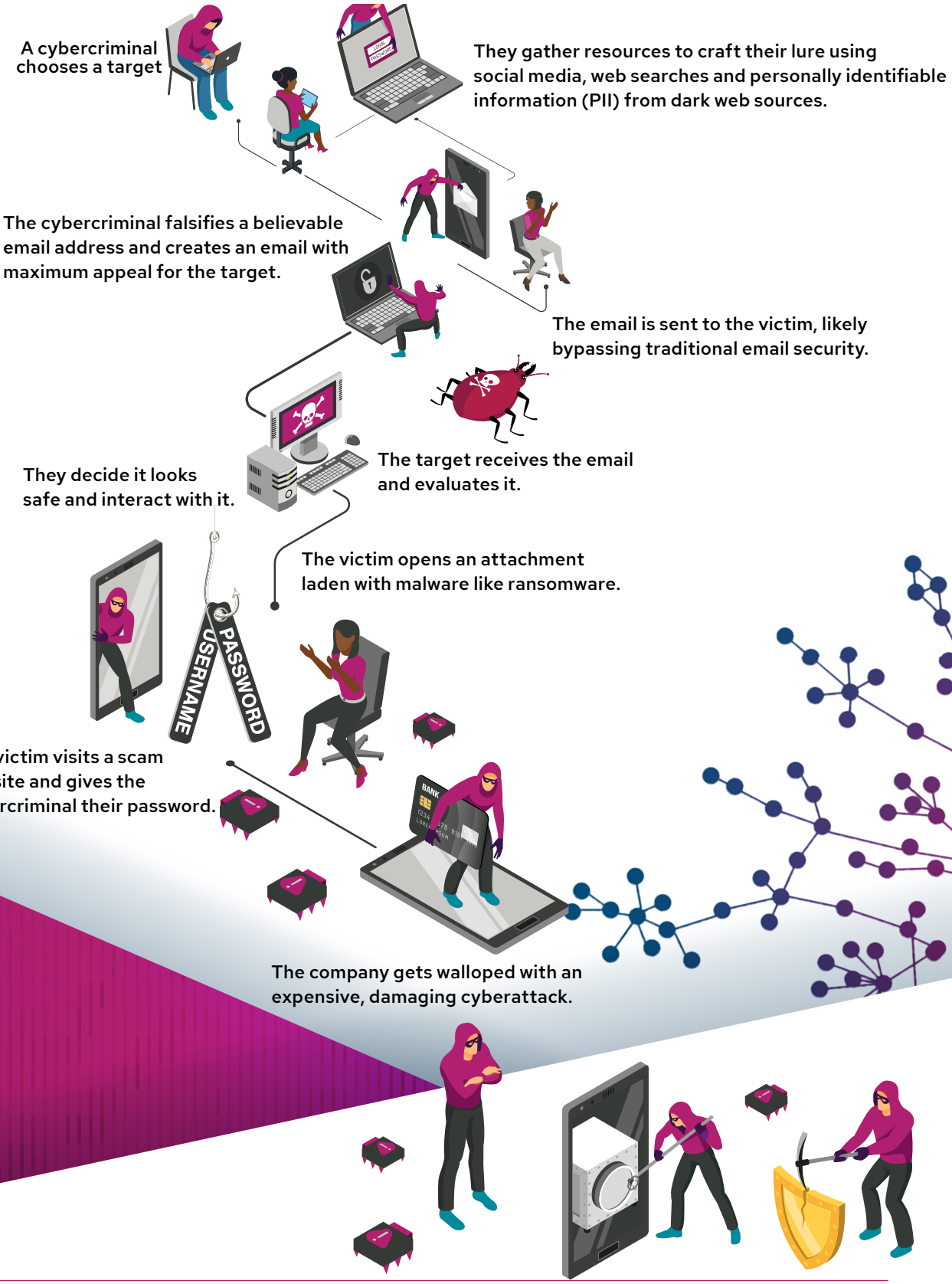
An **epic Twitter breach** resulted in the temporary takeover of more than 130 carefully chosen accounts, including celebrity accounts with a massive number of followers like Barack Obama, Bill Gates and Elon Musk. The attackers were then able to swindle $121,000 in Bitcoin through nearly 300 transactions by tweeting about a phony investment scheme – and it all started with a 16-year-old cybercriminal posing as a contractor phishing a privileged password from an administrator.

Cybersecurity giant **SolarWinds** experienced an intrusion by Russian nation-state cybercriminals who were then able to attach a few snippets of code on a routine patch. The patch was then distributed to and downloaded by major U.S. government agencies and national security assets open backdoors that gave the threat actors access to their systems and data for more than six months undetected. The breach was initially discovered by cybersecurity experts at FireEye and was determined to have started with a spear-phishing email.

A monster ransomware attack that hit **Blackbaud**, the leading developer of software used by non-profits for fundraising and administration, is still reverberating over a year later. The attack rocked more than 120 non-profits including Britain's National Trust, Human Rights Watch and National Public Radio. Adding to the complexity, many hospitals use Blackbaud's platform for fundraising, making this the biggest healthcare cyberattack in history. The point of entry for the ransomware was a phishing email.

ANATOMY OF A PHISHING ATTACK

An estimated **60%** of companies go out of business after a successful cyberattack. Here's how the cycle that ends in disaster starts.



ATTACK PROFILES

One major factor in the phishing boom has been a precipitate increase in the volume of email that businesses are handling. Of course, more email means more phishing, and cybercriminals didn't waste the opportunity to exploit the stresses of the global pandemic and record volumes of email use to facilitate cybercrime.

Workers handled 72% more emails in 2020 than in 2019.

Email is the primary form of communication for remote workers, and it became the primary way that business was conducted in 2020. Even in a world where in office meetings and face-to-face business deals are on the table again, **researchers who study corporate communications** do not expect that dependence to fade. Roughly 306.4 billion e-mails were estimated to have been sent and received each day in 2020, and this figure is expected to increase to over 376.4 billion daily emails by 2025.

No two phishing attacks are the same, but they can have similar characteristics. Cybersecurity experts have divided phishing threats into separate categories or profiles to better explain exactly how each scheme gets the dirty work done – and knowing what to look for gives you an edge that enables you to spot and stop phishing before an incident becomes a catastrophe.

ANGLER PHISHING

The Theme

A phishing attack conducted through the use of social media lures, like emails telling the target that they have been tagged in a photo or direct message by a recruiter.

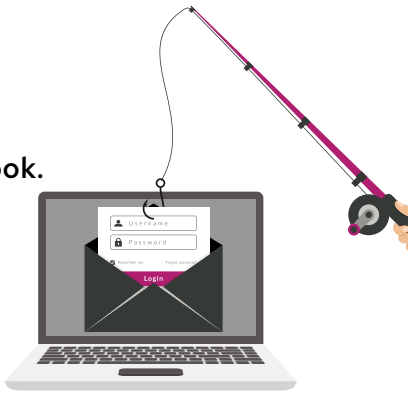
The Goal

Enticing the target to interact with a fake or spoofed login page for the requisite social media site that they can then use to capture the victim's password. The cybercriminals can then perform an ATO and use the victim's account for fraud like BEC or snoop for information on the victim's connections to help them better target sophisticated spear phishing attacks.

The Scam

Angler phishing is a relatively new form of phishing that has risen to prominence over the past decade. The preferred format for a malicious message using this technique is email, but it can also be conducted through messaging. LinkedIn messages are the most effective for cybercriminals, with a 47% open rate. **Some examples include:**

- **Recruiters are looking at your profile!**
- **You appeared in new searches this week!**
- **Please add me to your LinkedIn network.**
- **A new photo of you has been tagged on Facebook.**
- **Someone sent you a direct message on Twitter.**
- **See who is looking at your profile!**
- **Join my network on LinkedIn!**



The Damage

Victims that fall for this scam can have their social media accounts stolen or compromised. They are also at risk of identity theft. The companies that those victims work for should hope that their employees who fall for this scam aren't among the 60% of workers who use the same password for work and home applications.

BRAND IMPERSONATION

The Theme

A phishing attack that is conducted using carefully crafted or spoofed emails designed to trick the victims into believing they're legitimate messages from trusted entities. Variations of this scam include impersonating retailers, service providers, government agencies, charities or business partners.

The Goal

To acquire money, credentials, sensitive information or access to financial information from victims.

The Scam

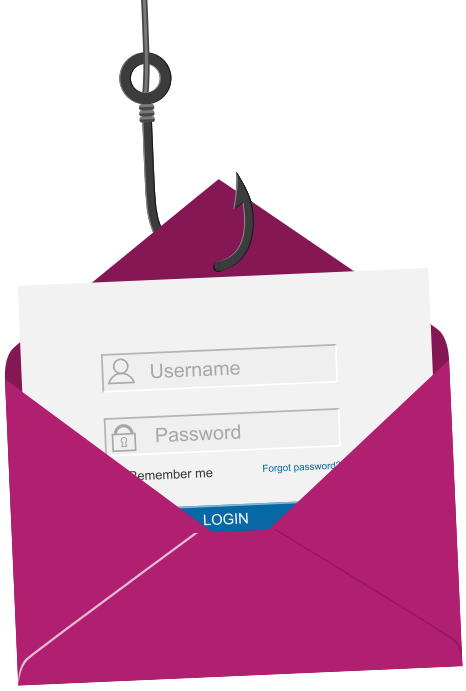
This variety of phishing offers the cybercriminal a wide variety of potential personas. Brand impersonation scams often make use of records from data breaches at the brand or similar entities acquired in dark web data markets and dumps as well as genuine emails from the brand to spoof.

They can include:

- **An alert that you need to login and patch a vulnerability from a software provider.**
- **A message asking for address confirmation for a shipment.**
- **Fundraising messages from a favorite charity.**
- **A routine message asking the target to reset a password at a shopping site.**
- **Inquiries from a professional organization that's updating its records.**
- **A survey that promises prizes for filling it out.**
- **A no tice from the city saying that you've underpaid your property tax.**
- **New terms and conditions from the phone company that you must click to acknowledge.**
- **An email about a special sale at your main supplier.**
- **An advertisement from a theme park where you've vacationed, offering deals.**

The Damage

This devious tactic opens businesses up to BEC, ATO, intrusions, malware, ransomware, data breaches and other nasty incidents. The most imitated brand of 2020 was Microsoft, which made up 45% of all brand impersonation attacks, followed by DHL and Amazon.



BUSINESS EMAIL COMPROMISE

The Theme

A phishing attack that uses fake emails to request payment from a business.

The Goal

Getting businesses to transfer money or provide sensitive financial information under false pretenses.

The Scam

The tricky part of spotting BEC attacks is that they're carefully crafted to be so believable that they fly right under the radar. They are primarily targeted to ensnare people within an organization who handle matters of payment or **can access funds quickly like:**

- **Administrative assistants who routinely process payments for small expenses.**
- **Executives who can order bills to be paid without oversight.**
- **Clerks who make vendor payments.**
- **Budget controllers who pay for recurring services.**
- **Accounting personnel who regularly renew licenses or pay government fees.**
- **Associates who regularly wire money to other companies**
- **Any employee who has access to spend or transfer funds.**

The Damage

BEC enables cybercriminals to get paid directly and capture financial information like banking accounts and executive credit card numbers to facilitate fraud and other financial damage.

RANSOMWARE/MALWARE

The Theme

A phishing attack that packs a punch by delivering a nasty software surprise.

The Goal

To infect computers with malicious software that enables cybercriminals to encrypt systems and data, making them inaccessible without a "key" obtained from the bad actors that did the deed.

The Scam

Malware and ransomware are weapons that can be wielded by cybercriminals against business, infrastructure, private and public sector targets. Some common ways malware and ransomware are used include:

- **Taking control of manufacturing, production or industrial equipment.**
- **Secretly copying data to a server controlled by cybercriminals.**
- **Installing payment skimmers to steal credit card numbers or divert online payment funds.**
- **Encrypting systems and data to disable operations and demanding a payment for the key.**
- **Snatching up important data like medical research, schematics, records, formulas or databases.**
- **Stealing sensitive data and threatening to release it on the dark web without a ransom payment.**
- **Shutting down internet-enabled systems, from transportation systems to IoT devices.**
- **Enabling hacking and intrusion by nation-state actors.**

The Damage

Malware and ransomware are the most dangerous results of phishing and can destroy infrastructure, harm research and development efforts, shut down production lines, drive a business into bankruptcy, facilitate espionage and terrorism, or even be used as a weapon of war.

SPEAR-PHISHING

The Theme

A phishing attack featuring personalized details in the lure that add believability to increase the likelihood that the recipient will take the bait.

The Goal

To lure unwary recipients into taking an action that compromises their credentials, obtains sensitive information or deploys malware (including ransomware).

The Scam

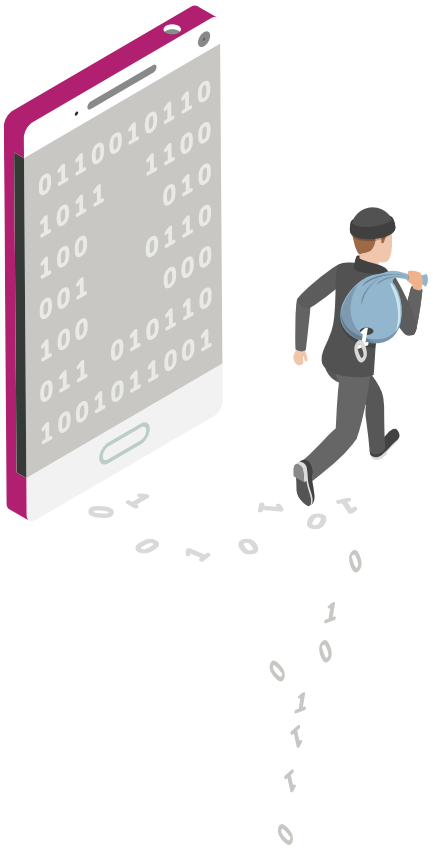
Cybercriminals use personalized information about their targets to craft emails that seem legitimate, often powered by information obtained from dark web markets and data dumps. **These lures can include:**

- **Emails from the recipient's alma mater asking for updated address information.**
- **A message advising the victim to reset their password at a social media site.**
- **Free downloads from organizations to which the recipient belongs.**
- **Requests for donations from charities that are in the recipient's sphere.**
- **Fake political emails from candidates or parties.**
- **Attachments like brochures or notices from trusted sources like a government agency.**
- **Spoofed messages from the recipient's regular service providers, suppliers or other vendors.**

The Damage

Spear-phishing is growing increasingly more dangerous as the amount of data available to cybercriminals allows them to create better bait. It is commonly used to capture credentials, steal information, cause a data breach, or deploy malware and ransomware.

WHALING/CEO FRAUD



The Theme

Whaling is a highly specialized spear-phishing attack that is crafted to perfectly imitate a company executive, or alternately, to fool a company executive into thinking that the message is from a trusted source.

The Goal

To lure an employee into performing an action like giving out a privileged credential, supplying sensitive information or transferring money without asking questions out of a desire to please the boss. Alternately, cybercriminals use this technique to convince executives that they are a trustworthy business associate who is owed money or is privy to proprietary data.

The Scam

Highly specific lures are crafted using personalized information about the target gathered from publicly available sources, harvested from social media sites and obtained from dark web markets and data dumps. Sometimes the cybercriminals will spoof legitimate messages or leverage a legitimate email account gained through BEC. **These lures can include:**

- **Emails from the recipient's bank, credit card company or a similar source.**
- **Invoices from contractors or freelancers.**
- **Updates from a software vendor.**
- **Charitable donation requests.**
- **Fake political emails from candidates or parties.**
- **Attachments like brochures or notices from trusted sources like a government agency.**
- **Spoofed messages from the recipient's regular service providers, suppliers or other vendors.**

The Damage

Whaling and CEO fraud aren't the most frequently conducted types of phishing because each operation requires extensive research and a high level of skill in crafting and delivery. Bad actors will frequently use brand impersonation in these attacks and usually favor posing as **Zoom, Amazon and DHL**.

THE NEXT BIG THING IS HERE – AFFORDABLE, AUTOMATED, ANTI-PHISHING SECURITY

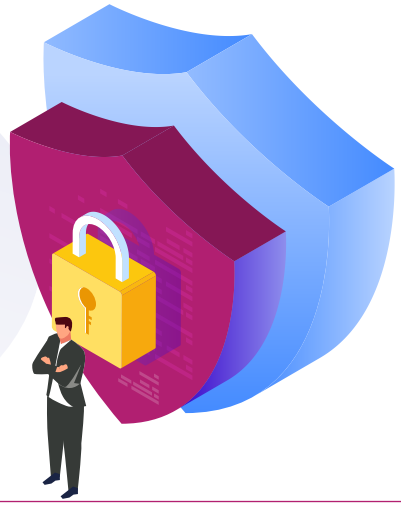
The FBI's IC3 report confirmed that phishing attacks are at their highest level in three years – and that number is only going up. Whether they're stealing credentials or deploying ransomware, one thing that all forms of phishing have in common is that they require human interaction to work. That means the best way to prevent employees from clicking on a phishing email is to prevent them from ever receiving it.

That's where Graphus comes in. As an AI-powered automated sentinel against phishing, this innovative solution provides businesses with three overlapping layers of smart protection based on a patented algorithm that spots and stops phishing email without disrupting your flow of communication.

The first layer of defense, **TrustGraph**, uses more than 50 points of comparison to determine the legitimacy of every incoming message.

The second layer, **EmployeeShield**, warns employees if a message from a new contact seems unusual, placing a warning banner at the top that enables them to mark it as safe or report it as phishing easily.

The final layer, **Phish911**, adds everyone to the cybersecurity team by empowering employees to reject suspicious messages with just one click, immediately quarantining them for all recipients pending inspection by the IT team.



GET BIG BENEFITS FOR A SMALL PRICE

Graphus takes care of many routine activities, freeing up techs to focus on complicated tasks that require human ingenuity. This always-on guardian never takes a day off, continually providing your business with useful benefits that enhance your cybercrime protection at a great price.

SAVE TIME AND MONEY WITHOUT LIFTING A FINGER

With Graphus, techs no longer need to jump at every suspicious message to prevent someone else from opening it, thereby saving time and increasing productivity. If any employee rejects a message, it is automatically removed from everyone's inbox until an IT team member determines it is safe. Automatic quarantine and capture features reduce your help desk's caseload by up to 80%.

No need to spend time uploading threat reports or finding the latest patch to make sure you're protected against new threats. The AI gathers its own intelligence and never stops learning, constantly refining your protection to meet the needs of your unique business in a rapidly evolving threat landscape.

Smart technology means fewer headaches for everyone. Alerts and false positives are minimized in the user friendly operations center. Simple deployment and non-fussy integrations mean that it doesn't take hours to set up. In fact, your protection from phishing will be up and running in minutes.

The biggest benefit? Graphus catches 40% more phishing messages than the competition and outperforms old-fashioned secure email gateways (SEGs) at every turn, giving your business cutting-edge protection that keeps you a step ahead of cybercriminals.

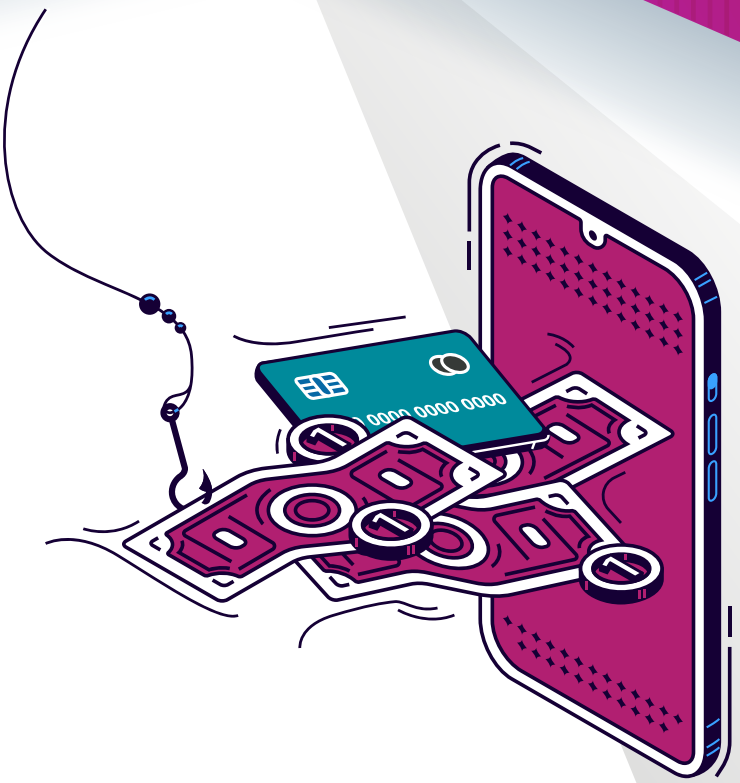
GO TO THE HEAD OF THE CLASS

Reducing your organization's phishing risk has never been more important, and we make it easy. Put Graphus to work for your business to gain strong protection against today's biggest threats and peace of mind – because it's time to stop worrying about phishing and start worrying about more important things like growing your business.

SCHEDULE A DEMO

LEARN MORE

SEE GRAPHUS IN ACTION



GRAPHUS
A Kaseya COMPANY