

Don't Take the Bait

Phishing is big business. Don't get hooked.

In the last year, phishing attacks have seen a meteoric rise as attackers continue to refine tactics and share successful types of attacks. In particular, they've taken advantage of the malware-as-a-service offerings on the dark web in order to increase the efficiency and volume of attacks. In fact, 41% of organization now report at least daily phishing attacks.¹

In this paper, we'll dive into the evolution of phishing in recent years, how it works, and what it looks like. And as cybercriminals continue to prey on employees through their technology, we'll make an argument for the importance of a multi-layered defense against phishing attacks: combining advanced security technologies with educated, phishing-aware employees.

More than annoying spam

Traditionally phishing was associated with online banking cybercrimes: crooks send an email luring you to a website that's a visual clone of your bank's login page, where you enter your credentials into a phony form and drop them right into the criminals' laps.

But phishing covers much more than just fake banking sites and links to life-enhancing pills or package deliveries: it's really just about dangling bait in front of you and waiting for you to swallow it, providing them with useful and valuable information.

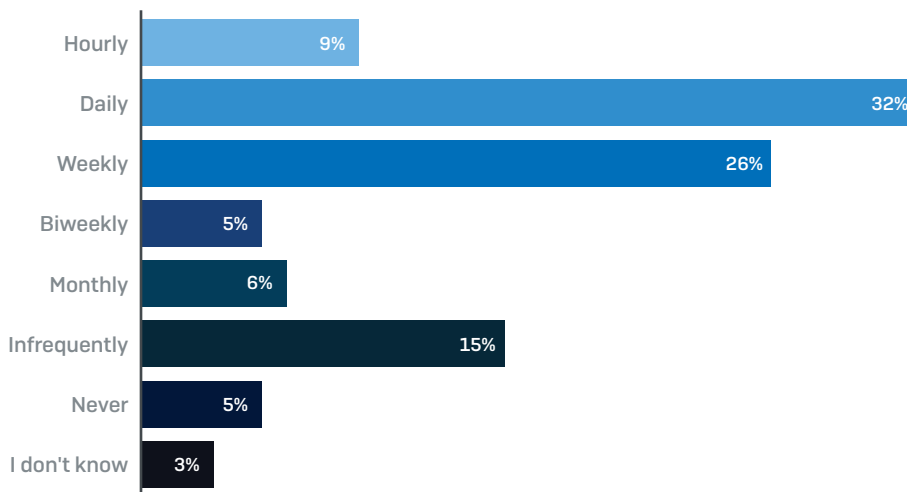
93%
of data breaches
include phishing²

Phishing is big business

In recent years, the volume of phishing attacks has grown dramatically, fuelled by dark web services such as free phishing kits and phishing-as-a-service. It's become increasingly simple for even the least technically inclined attacker to leverage advanced malware that's been produced by someone far savvier than they are.

As a result, phishing attacks are now a regular part of daily life. 41% of IT professionals report that their organization experiences at least daily phishing attacks, while over three-quarters (77%) experience attacks at least every month.³

Frequency of phishing attacks

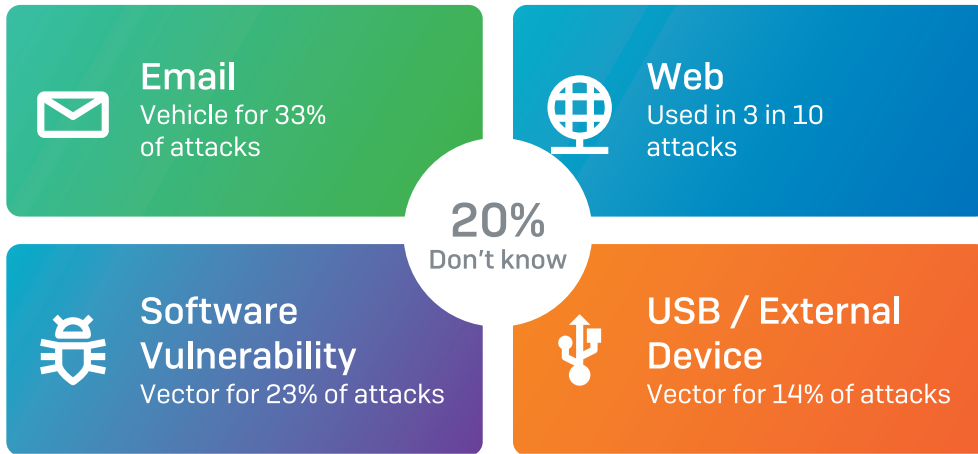


The most common attack vector

A recent survey of 3,100 organizations revealed that email is the most common attack vector, used in 33% of successful cyberattacks. It's also a highly effective vector: 53% of organizations that had been hit by a cyberattack in the last year were victims of phishing.⁴

Phishing emails are often the first stage in a complex, multi-technique attack. For example, clicking on a link in a phishing email connects through to a command and control server, which then infects the organization with malicious software.

1 in 3
cyberattacks entered
the organization
via email



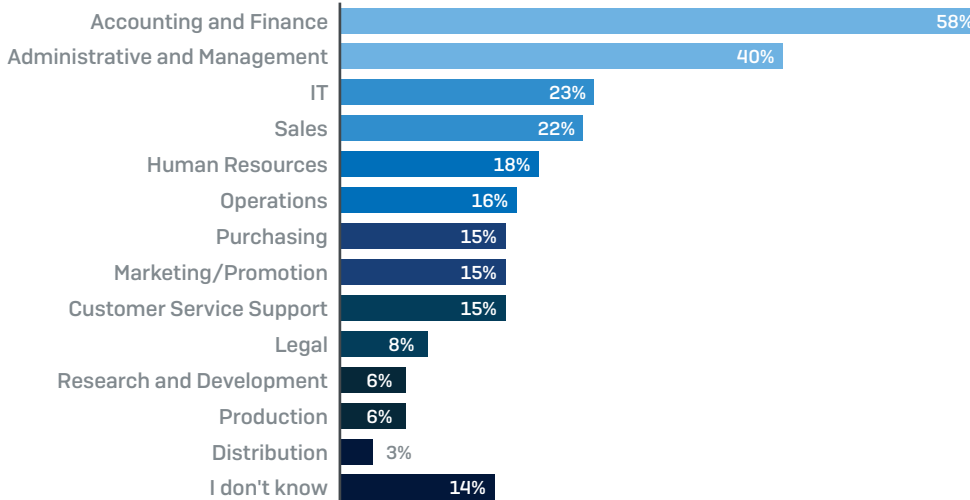
How the most recent cyberattack to affect an organization got in - Sophos survey of 3,100 IT Managers.

The main driving force behind phishing attacks is financial gain. The Verizon 2018 Data Breach Investigations Report revealed that:

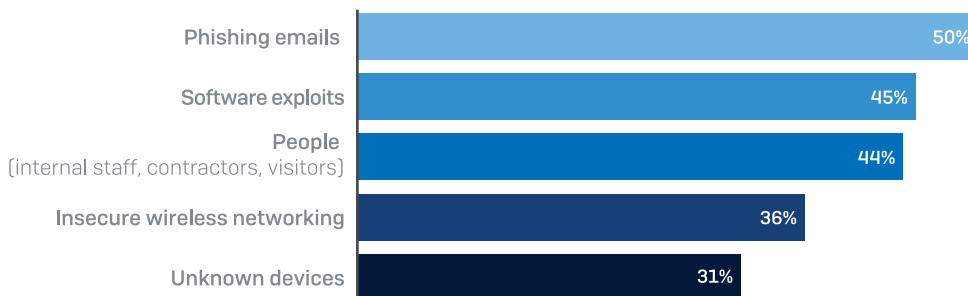
- ▶ **59% of attacks are motivated by financial gain.** This includes harvesting credentials for resale on the dark web, infecting systems with ransomware, or impersonating senior managers to convince employees to transfer funds or valuable data.
- ▶ **41% of attacks aim to gain unauthorized system access.** Examples including obtaining access to a company's network to steal data, or gain control of systems.

Given the financial motives behind most attacks, it's unsurprising that cybercriminals often targeting employees who have access to company finances, tricking them into making financial transfers to bank accounts controlled by the criminals. However, they also target those who manage business processes and IT controls, opening organizations up to a range of attacks including ransomware and extortion.⁵

Departments most targeted by phishing attacks



It's therefore unsurprising that phishing is considered the most significant security risk by IT managers, with 50% ranking it as a top-three risk. Furthermore, in third position on the risk list is people, which includes internal staff, contractors and visitors. This reflects the growing trend with cyber criminals to exploit human weaknesses and behaviors in their attacks.



*What/who do you consider to be your organization's top three security risks?
Combination of responses ranked first, second and third. 3,100 respondents.*

Improving efficiency and productivity

Currently, 89% of phishing attacks are carried out by organized crime. As phishing is run like a business, attack strategies have evolved in ways we can all identify with: how can I make my job easier and work more efficiently, and how can I expand in order to increase profits?

This has given rise to more efficient attack distribution methods, with on-demand phishing services, off-the-shelf phishing kits, and new waves of attack types such as Business Email Compromise (BEC) that look to target higher value assets via social engineering.

Free phishing kits

Ever wanted your products to sell like the latest iPhone? For most of us, if we see an idea that works well – from a friend, colleague or competitor – we're tempted to "borrow" the idea for ourselves, right? Well, the phishing community is no different. Actually, it's better organized.

An interesting facet of the phishing ecosystem is that there are a large number of actors committing attacks, but only a small number of phishers that are sophisticated enough to write a phishing kit from scratch. Because of this, phishing kits are now widely available for download from dark web forums and marketplaces, and give attackers all the tools they need to create profitable phishing attacks: emails, web page code, images, and more.

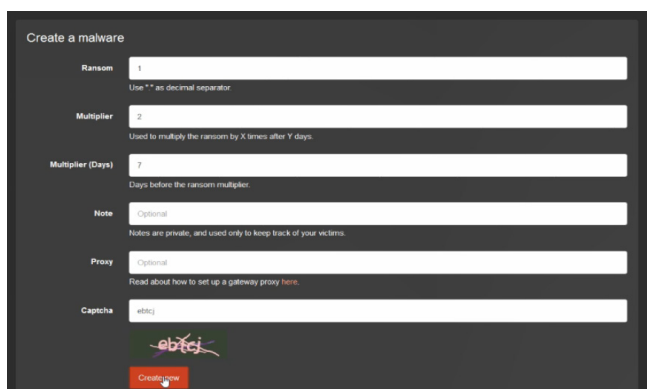
Kit authors seek to profit by distributing their kits to these less sophisticated users, making money in one of two ways: offering free kits containing backdoors for the author to collect any data collected by the sender, or selling kits for profit. The highest priced kits now even contain features like campaign tracking control panels.

89%
of phishing attacks
orchestrated
by professional
organized crime

Attacks-as-a-service

In fact, attackers don't even need to know how to create malware or send emails anymore. As-a-service and pay-as-you go solutions permeate most online service technologies, and phishing is no different – with a range of services increasingly available to attackers:

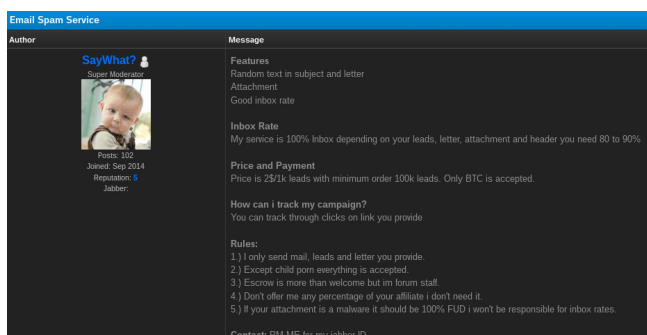
- **Ransomware-as-a-service** allow a user to create an online account and fill out a quick web form, including the starting ransom price and a late payment price for victims. The provider of the service then takes a cut of each ransom paid, with discounts offered if the user is able to translate the malware code into new languages or if the volume of the attack exceeds a certain level.



The screenshot shows a web form titled "Create a malware" with a dark background. It contains several input fields: "Ransom" (with a value of 1 and a note "Use '' as decimal separator"), "Multiplier" (with a value of 2 and a note "Used to multiply the ransom by X times after Y days"), "Multiplier (Days)" (with a value of 7 and a note "Days before the ransom multiplier"), "Note" (with "Optional" and a note "Notes are private, and used only to keep track of your victims."), "Proxy" (with "Optional" and a note "Read about how to set up a gateway proxy here."), and "Captcha" (with a value of "e8fbcj"). A red "Create" button is at the bottom.

Satan ransomware - an online service allowing crooks to create their own virus in minutes and start infecting Windows systems.

- **Phishing-as-a-service** allows users to pay for phishing attacks to be sent for them, using global botnets to avoid known dodgy IP ranges. Guarantees are even made to only bill users for delivered email messages, much like any legitimate email marketing service.



The screenshot shows a forum post titled "Email Spam Service". The author is "SayWhat?" (Super Moderator) with a profile picture of a baby. The message content includes: "Features: Random text in subject and letter, Attachment, Good inbox rate"; "Inbox Rate: My service is 100% inbox depending on your leads, letter, attachment and header you need 80 to 90%"; "Price and Payment: Price is 250k leads with minimum order 100k leads. Only BTC is accepted."; "How can I track my campaign?: You can track through clicks on link you provide"; "Rules: 1.) I only send mail, leads and letter you provide. 2.) Except child porn everything is accepted. 3.) Escrow is more than welcome but im forum staff. 4.) Don't offer me any percentage of your affiliate I don't need it. 5.) If your attachment is a malware it should be 100% FUD I won't be responsible for inbox rates."; "Contact: PM ME for my jabber ID".

Spam sending service example - priced per email sent to an activate mailbox, with tracking even available on click-through rates.

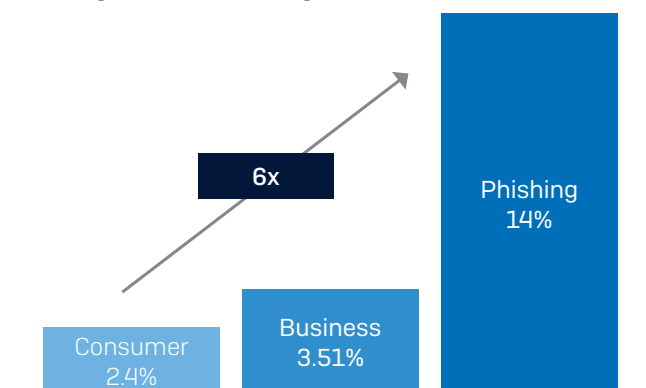
These services have led to the explosion of phishing attacks highlighted earlier, as any attacker can launch an attack regardless of technical skill.

Like marketing, only six times better

Most worryingly of all, these dark web services have freed up attackers' time so that they can concentrate on refining their campaigns and honing their nefarious skills.

And their tactics are allowing them to achieve the kind of results most sales and marketing teams would be jealous of, with phishing emails currently six times more likely to be clicked than regular consumer marketing emails.⁶

Phishing email click through rates



This newly-found research and development time has kicked phishing threats up a notch. Business Email Compromise (BEC) attacks are on the rise – a dangerous subset of phishing attacks that enable attackers to expand profit areas by targeting high value corporate targets.

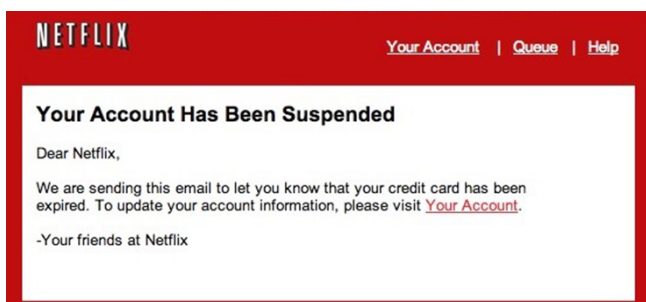
How phishing works

As mentioned, phishing covers more than just fake banking emails and package delivery alerts. It's about convincing you to provide something valuable to the attackers. And what started off as simply "phishing" has now developed into three branches of attacks: the classics, mass phishing and spear phishing, and Business Email Compromise, subset of spear phishing.

Mass phishing

These attacks are largely opportunistic, taking advantage of a company's brand name to try and lure the brand's customers to spoofed sites where they are tricked into parting with credit card information, login credentials, and other personal information that will be later resold for financial gain.

- Targeting the assets of individuals
- Typically consumers of a brand's products or services
- Impersonal batch and blast
- Focused on stealing personal data, such as login credentials

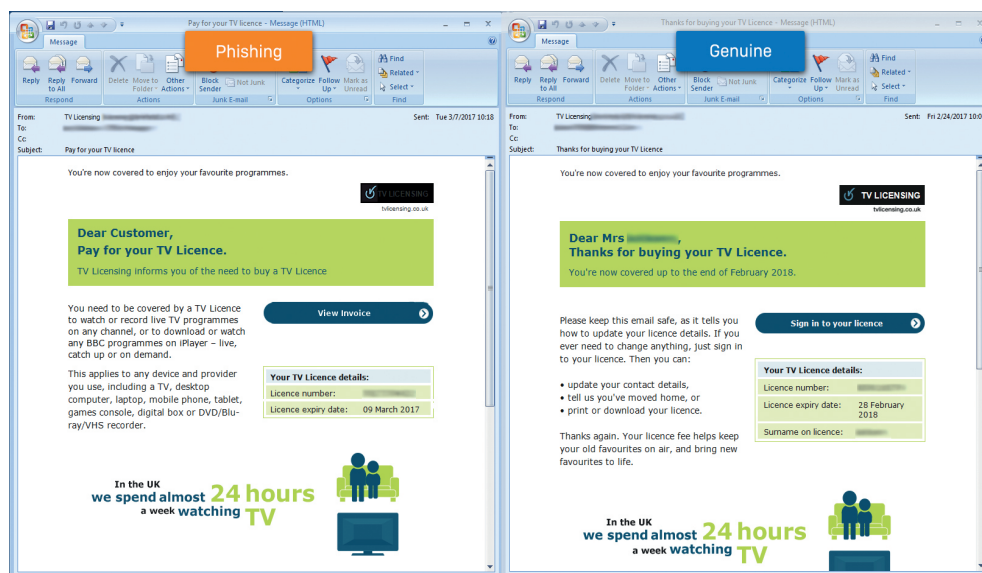


A typical 'verify you account' mass phishing example

Spear phishing

The other kind of threat is of the spear phishing variety, where emails impersonating a specific sender or trusted source are sent to targeted individuals within organizations to try to get them to take certain actions, like sending money to spurious accounts.

- ▶ Targeting the assets of a specific organization
- ▶ Typically an individual or specific group in an organization
- ▶ Spoofed (look-a-like) email addresses to aid conversion
- ▶ Impersonates trusted sources and senior executives



Genuine and phishing emails are often very similar, as shown in this convincing UK TV Licence example.

Spear phishing attacks are increasingly common and cybercriminals continue to refine their techniques in order to increase effectiveness. In a recent survey of 330 It professionals, 55% confirmed that that their senior managers had been impersonated in spear phishing attacks.⁷

More targeted subsets of spear phishing use social engineering to gather target data and increase conversion. These are known as CEO Fraud, Whaling, and most recently, Business Email Compromise (BEC).

Business Email Compromise

Business Email Compromise attacks are so-named because they're associated with employee email accounts being compromised rather than the sender address being spoofed. This makes attacks much harder to spot by end users.

- Targeting corporate information, access credentials, or funds from a company
- After attackers choose an organization to target, they will locate individuals within that business to attack by gathering data from sites such as Facebook and LinkedIn in order to construct highly targeted and believable phishing emails
- The attacker then isolates that individual by making the email message appear to be from a high-level exec and will add time pressure, typically sending messages at the very end of the day or week

Unlike mass or spear phishing campaigns, these attacks regularly target company funds. And unlike attacks from earlier years that would provide destination bank account information to would-be victims in PDF attachments, BEC attacks hold back such information until a positive response has been sent by the victim. After all, a fraudulent account will be the attacker's biggest expense in the attack, so it's an important asset to guard as it could be provided to the authorities if the victim realized the ruse early on.

BEC attacks are altogether harder to spot since the attackers compromise corporate email accounts to send from. In fact, the latest FBI figures show that a staggering number of businesses are now falling for these kinds of attacks, with losses in 2016 reaching \$3.1 billion across 22,000 enterprises.

Evolving Phishing Techniques

Phishing techniques continue to evolve. As people become more attuned to too-good-to-be-true emails with fabulous prizes, the crooks are moving towards simple, mundane emails that are less likely to stand out.

This research here shows the top 10 emails that people fell for in Sophos' Phish Threat simulation training. As you can see, these are all very 'normal' email subject lines – topics that don't usually raise any eyebrows.

| EMAIL SUBJECT | % OPENED AND CLICKS |
|---|---------------------|
| [Jira] A task was assigned to you | 39% |
| Let's meet next week | 29% |
| Harassment Awareness Training | 26% |
| Car lights left on | 25% |
| eFax message from {Customer Name} - 2 page(s) | 24% |
| Traffic Citation for {Email First Name} {Email Last Name} | 22% |
| In arrears for driving on toll road | 21% |
| Suspicious male spotted outside {Customer Name} Building | 20% |
| PLEASE READ - Annual Employee Survey | 19% |
| New Email System at {Customer Name} -- Please Read | 18% |

\$140K
Average loss
per scam

Don't Take the Bait

The most effective phishing email referenced JIRA, a popular software tool, followed by a meeting request or a harassment training email – designed to make the recipient panic and not go through usual security checks!

Sample phishing simulation emails

Samantha,

A number of employees have been asked to attend a **mandatory harassment awareness training**. If you have not been asked to attend this training by your supervisor, please use the **attached word document** to confirm that your attendance is not required.

Best regards,

Human Resources Department

To all employees,

Someone left their headlights on in the parking lot. An employee took [a picture of the car that I've uploaded here](#). Please check to see if this car is yours, as we don't want anyone leaving work today only to find their battery is dead!

Thanks again everyone.
Amena Adnan
Building Manager

Spot the signs

So, those fake invoices that arrive telling you that someone bought an airline ticket on your credit card, and to please open the attached document for details if you want to dispute payment? That's mass phishing.

So are those fake courier notes that say they need you to confirm your company's address so that an undelivered item can be shipped.

Spear phishing, for the most part, is very much the same thing, except that the bait is more specific. Or, in the case of BEC attacks, the message may contain no malicious links or attachments but rather ask you to transfer funds – making the attack seem more believable.

Simply put, if a fraudulent email starts "Dear Customer," it's phishing. But if it salutes you by your name, it's spear phishing. And if it's from your boss's actual email address, it's a Business Email Compromise (BEC) attack.

Of course, many spear phishing attacks are much more pointed than that, if you will excuse the metaphor. Well-prepared crooks may know your job title, your desk number, the sandwich shop you often visit for lunch, the friends you hang out with, your boss's name, your previous boss's name, and even the name of the supplier of your company's coffee beans.

And, as you can probably imagine, when it comes to spear phishing, nothing breeds

30%
of phishing emails
are opened

Don't Take the Bait

success like success. The more that crooks, cybergangs, or teams of state-sponsored actors learn about your company, the more believable their phishing attempts will appear.

This information can be acquired in many ways, including:

- Previous successful attacks, such as data-stealing malware
- Private company documents, such as phone directories or organizational charts that show up in search engines
- Your personal and company social networking pages
- Disgruntled former employees
- Data bought from other crooks on the dark web

You can probably think of many other ways that "secret" information can become anything but secret. The bottom line is that understanding these tactics can mean you successfully avoid opening one of the 30% of phishing emails that are opened today.

Use this handy acronym to help your users spot the signs of a phishing email:

P: Promises unbelievable things

H: Harasses you to reply

I: Insists you act now

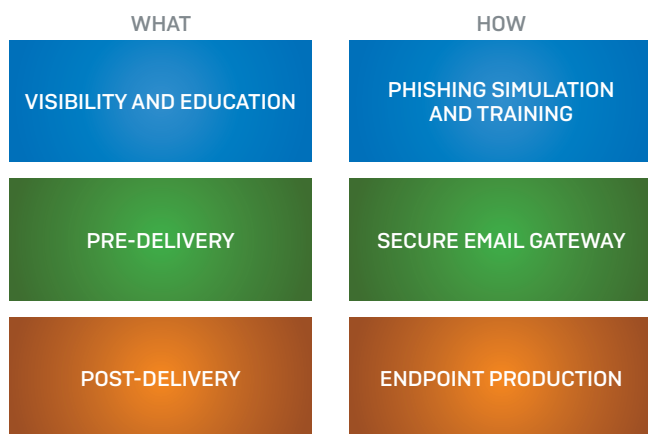
S: Sense of urgency

H: Hit delete!

If in doubt, report it to your IT team and hit delete to make everyone else in the company aware of the phish!

The fight against phishing

Phishing attacks come in all shapes and sizes, and unfortunately there is no silver bullet to stop phishing. A multi-layered defense against phishing attacks, combining advanced security technologies and educated, phish-aware employees, is the only answer. At Sophos, we recommend all organizations adopt a three-pronged approach:



1. Visibility and Education

Don't Take the Bait

In the fight against phishing, your users are the weakest link. In fact, it takes on average just 16 minutes for someone to click on a phishing email [Source: Verizon 2018 Data Breach Investigation Report].

- With your users at the front line of phishing attacks, it's essential to raise awareness and train people on how to spot – and avoid – phishing emails. There are three stages to an effective **phishing simulation and training** program:

TEST

Send simulated phishing emails emulating real-life tactics to test user awareness

TRAIN

Educate users on how to spot and stop the real thing

MEASURE

Track progress and improvement to demonstrate ROI and guide further training

2. Pre-Delivery

58% of email is spam and 77% of all spam emails contain a malicious file⁶. As a result, a **secure email gateway** is an essential element in your fight against phishing, trapping phishing emails before they can reach your inboxes. Core technologies to look for include:

- **Anti-spam:** Powerful spam traps across the globe stop emails from reaching your users.
- **Sender reputation:** IP reputation filtering to block unwanted emails at the gateway.
- **Sender authentication:** Detect sender spoofing, header anomalies, and suspect email body content.
- **Sandboxing:** Detonate suspicious files outside the network.
- **Malicious URL blocking:** Filter bad links, including protection against stealthy, delayed threats.

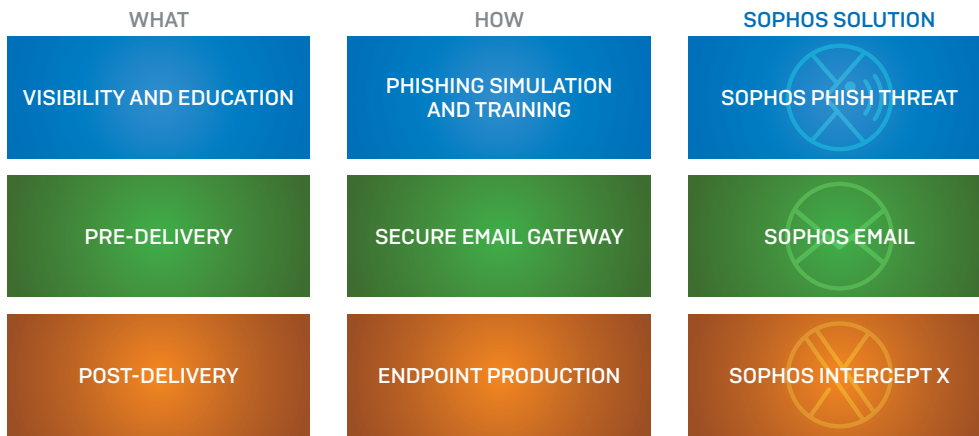
3. Post-Delivery

- Post-delivery is your final line of defense, protecting your organization if a user clicks a malicious link or open an infected attachment. Look for an **endpoint security** solution that offers both foundational and modern techniques, including:
 - **Deep learning:** Block never-before-seen threats from running in your organization.
 - **Anti-exploit:** Prevent attackers from exploiting vulnerabilities in legitimate software.
 - **Anti-ransomware:** Stop unauthorized encryption of your company resources.

How Sophos Can Help

Sophos is the only vendor to offer complete phishing protection – visibility and education,

pre-delivery, and post-delivery – all managed through a single web-based platform.



31%
reduction in employee susceptibility with Sophos Phish Threat

Sophos Phish Threat educates and tests your end users through automated attack simulations, quality security awareness training, and actionable reporting metrics. And it works: On average, customers see a 31% reduction in employee susceptibility after just four Phish Threat training emails.

With **Sophos Email**, you can trust your inbox again. It blocks phishing imposters and protects employees from attacks using fraudulent email addresses that impersonate trusted contacts. A combination of SPF, DKIM, and DMARC authentication techniques and email header analysis allows you to identify and permit legitimate emails while blocking imposters.

Sophos Intercept X combines a wide range of both foundational and modern (next-gen) techniques to the widest range of ransomware attacks and malware. Its deep learning neural network is training on hundreds of millions of malicious files to proactively detect unknown threats.

Unique to Sophos, you can manage all your phishing prevention technologies through a single web-based platform. This is called Sophos central. It is all web-based meaning there is no maintenance of servers and can be accessed anytime, anywhere saving time.

Start with one product and then add others whenever you are ready.

Don't Take the Bait

1, 3, 5, 7 Source: Phishing Temperature Check, Freeform Dynamics in association with The Register and Sophos, 2017

2 Source: Verizon 2018 Data Breach Investigations Report

4 The impossible puzzle of cybersecurity, Sophos, July 2019

6 Source: Verizon 2016 DBIR & Experian Email Benchmark Report Q4 2016

7 Source: SophosLabs, 2017

United Kingdom and Worldwide Sales

Tel: +44 (0)8447 671131

Email: sales@sophos.com

North American Sales

Toll Free: 1-866-866-2802

Email: nasales@sophos.com

Australia and New Zealand Sales

Tel: +61 2 9409 9100

Email: sales@sophos.com.au

Asia Sales

Tel: +65 62244168

Email: salesasia@sophos.com

© Copyright 2019. Sophos Ltd. All rights reserved.

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are
trademarks or registered trademarks of their respective owners.

2019-08-01 WP-UK (PC)

The logo for Sophos, consisting of the word "SOPHOS" in a bold, blue, sans-serif font.