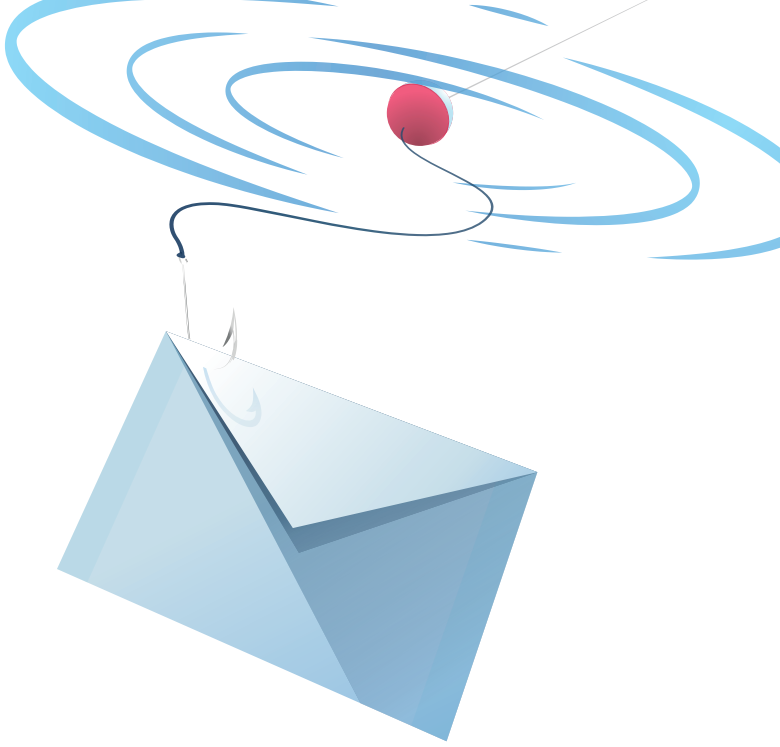
SOPHOS
Cybersecurity made simple.



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% organizations 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.

A Sophos Whitepaper June 2018

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.

93%
of data breaches include phishing[2]

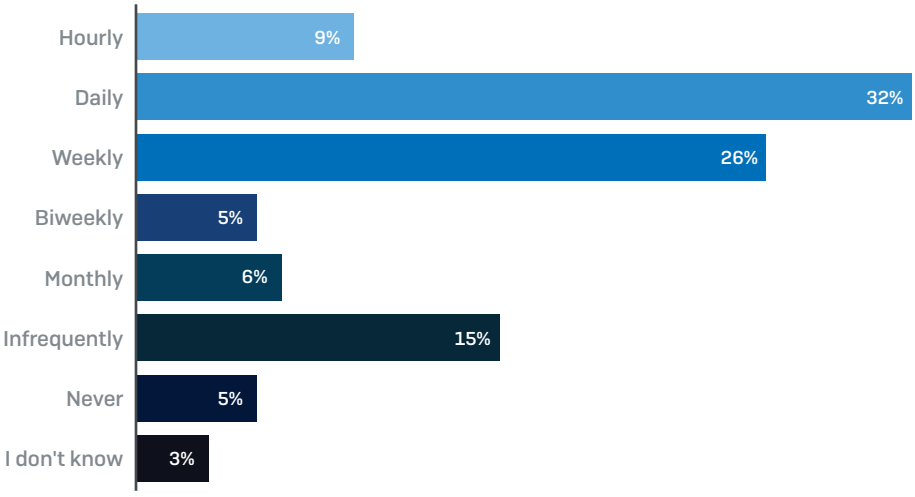
But phishing covers much more than just fake banking sites and links to life-enhancing pills or package deliveries: it's really just about dangling bait in front of you and waiting for you to swallow it, providing them with useful and valuable information.

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

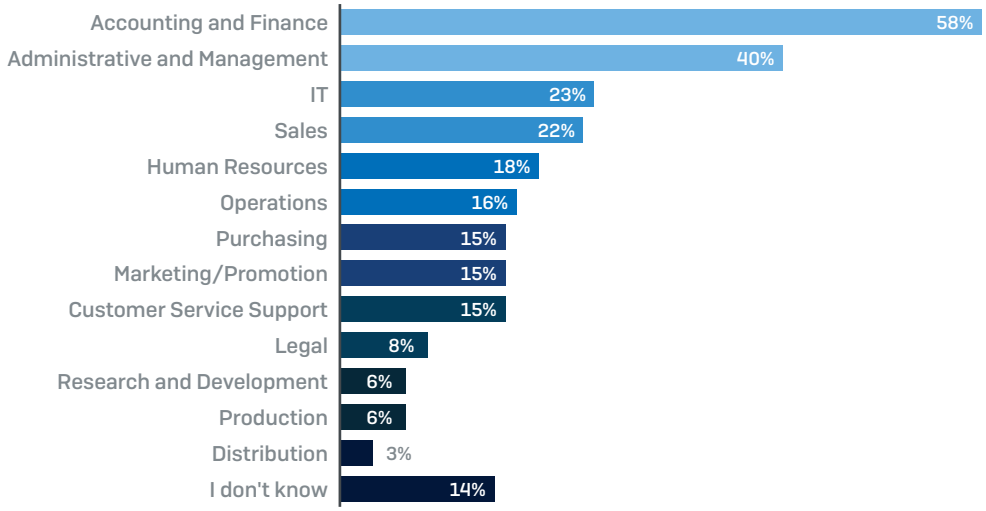


The main driving force behind phishing attacks is financial gain. The Verizon 2018 Data Breach Investigations Report revealed that:

- **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.[4]

Departments most targeted by phishing attacks



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?

89%
of phishing attacks orchestrated by professional organized crime

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.

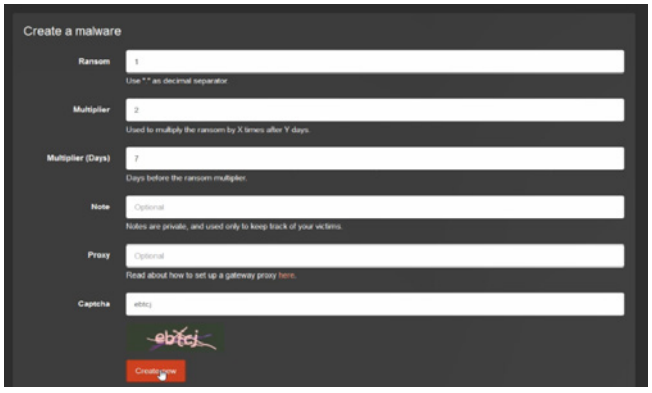
An interesting facet of the phishing ecosystem is that there are a large number of actors committing attacks, but only a small number of phishers that are sophisticated enough to write a phishing kit from scratch. Because of this, phishing kits are now widely available for download from dark web forums 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.

Attacks-as-a-service

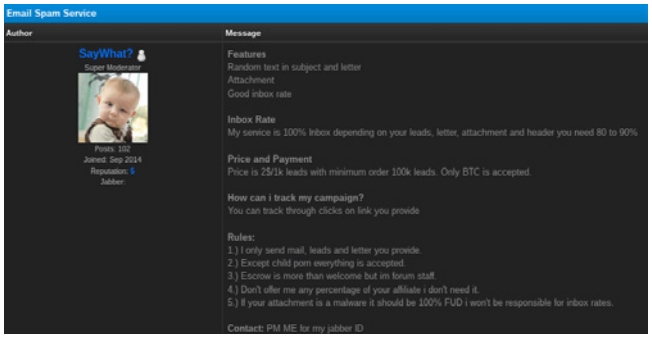
In fact, attackers don't even need to know how to create malware or send emails anymore. As-a-service and pay-as-you go solutions permeate most online service technologies, and phishing is no different – with a range of services increasingly available to attackers:

- **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.



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.



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

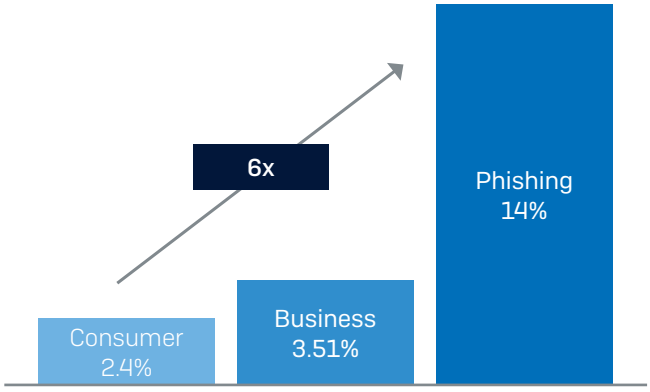
These services have led to the explosion of phishing attacks highlighted earlier, as any attacker can launch an attack regardless of technical skill.

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.[5]

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

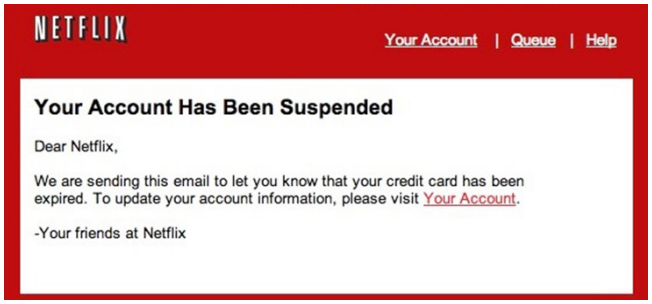
As mentioned, phishing covers more than just fake banking emails and package delivery alerts. It's about convincing you to provide something valuable to the attackers. And what started off as simply "phishing" has now developed into three branches of attacks: the classics, mass phishing and spear phishing,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

$3.1B
in losses from BEC attacks in 2016

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

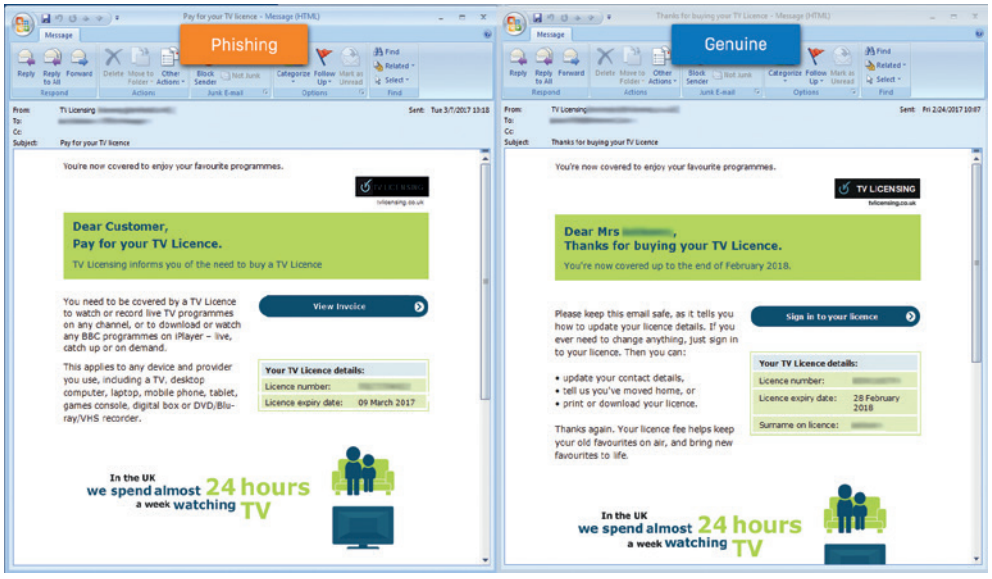


A typical 'verify you account' mass phishing example

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 License 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.[6]

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.

$140K
Average loss per scam

- 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.

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.

30%
of phishing emails are opened

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 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.

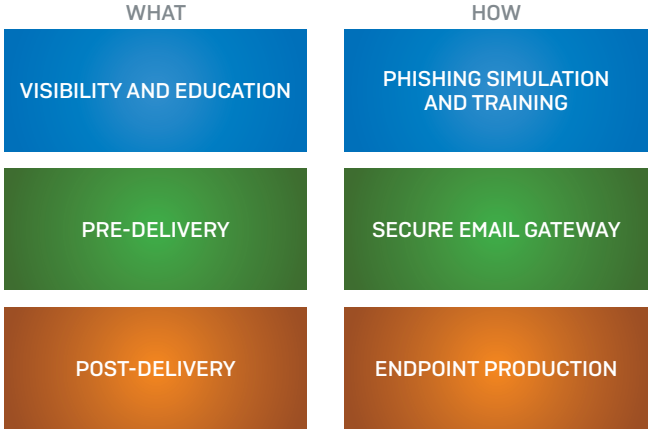
This information can be acquired in many ways, including:

- 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.

The fight against phishing

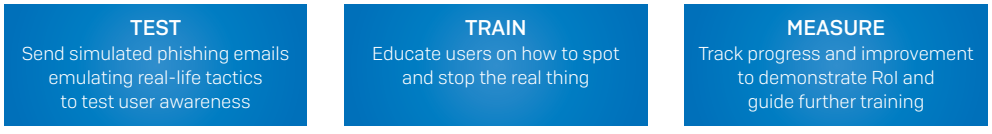
Phishing attacks come in all shapes and sizes, and unfortunately there is no silver bullet to stop phishing. A multi-layered defense against phishing attacks, combining advanced security technologies and educated, phish-aware employees, is the only answer. At Sophos, we recommend all organizations adopt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



1. Visibility and Education

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:



2. Pre-Delivery

58% of email is spam and 77% of all spam emails contain a malicious file[6]. 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:

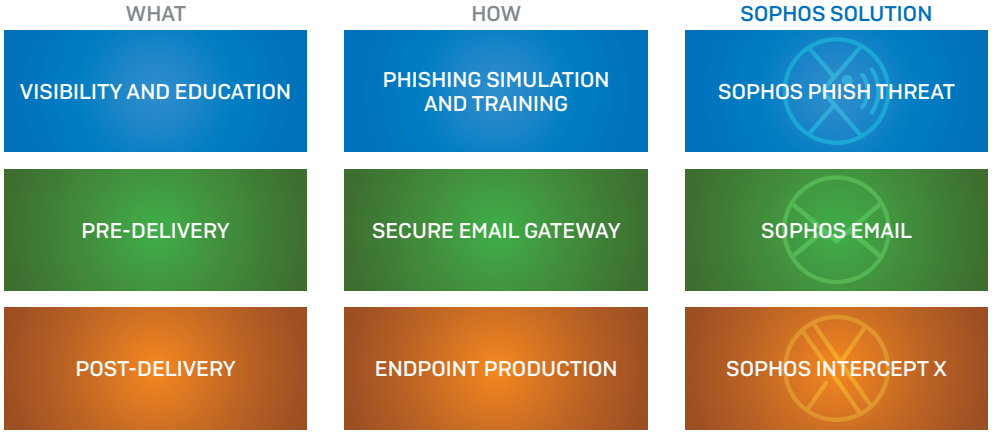
- **Anti-spam:** Powerful spam traps across the globe stop emails from reaching your users.
- **Sender reputation:** IP reputation filtering to block unwanted emails at the gateway.
- **Sender authentication:** Detect sender spoofing, header anomalies, and suspect email body content.
- **Sandboxing:** 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.



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. Learn more and try for yourself at www.sophos.com/phish-threat.

31%
reduction in employee susceptibility with Sophos Phish Threat

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. Learn more and take a test drive at www.sophos.com/email.

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. See for yourself at www.sophos.com/intercept-x

Unique to Sophos, you can manage all your phishing prevention technologies through a single web-based platform, Sophos Central:

- Save time and effort by managing everything through a single console
- Web-based, so there are no servers to maintain or manage
- Access anytime, anywhere
- Products are actively engineered to work together – no extra work to make them play nicely

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

Ten Tell Tale Signs of Phishing

The "tells" you can look for to help suss out potential scams.

1. **It just doesn't look right.** Is there something a little off with a particular email message? Does it seem too good to be true? Trust your instincts.
2. **Generic salutations.** Instead of directly addressing you, phishing emails often use generic names like "Dear Customer." This use of impersonal salutations saves the cybercriminals time.
3. **Links to official looking sites asking you to enter sensitive data.** These spoofed sites are often very convincing, so be aware of what personal information or confidential data you're being asked to reveal.
4. **Unexpected emails that use specific information about you.** Information like job title, previous employment, or personal interests can be gleaned from social networking sites like LinkedIn and is used to make a phishing email convincing.
5. **Unnerving wording.** Thieves often use unnerving wording (such as saying your account has been breached) to trick you into moving fast without thinking and in doing so, revealing information you ordinarily would not.
6. **Poor grammar or spelling.** This is often a dead giveaway. Unusual syntax is also a sign that something is wrong.
7. **Sense of urgency.** "If you don't respond within 48 hours, your account will be closed." By creating a sense of urgency, the thieves hope you'll make a mistake.
8. **"You've won the grand prize!"** These phishing emails are common, but easy to spot. A similar, trickier variation asks you to complete a survey (thus giving up your personal information) in return for a prize.
9. **"Verify your account."** These messages spoof real emails asking you to verify your account. Always look for signs of phishing, and always question why you're being asked to verify – there's a good chance it's a scam.
10. **Cybersquatting.** Often, cybercriminals will purchase and "squat" on website names that are similar to official websites in the hopes that users go to the wrong site e.g. www.google.com vs. www.g00gle.com. Always take a moment to check out the URL before entering your personal information.

For more tips and tools to stop phishing, visit www.sophos.com/prevent-phishing

1, 3, 4, 6 Source: Phishing Temperature Check, Freeform Dynamics in association with The Register and Sophos, 2017

2 Source: Verizon 2018 Data Breach Investigations Report

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

6 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

2018-05-31 WP-UK (3017-DD)

SOPHOS