SOPHOS
Security made simple.

CYGNUS SYSTEMS, INC.
Keeping IT Real

# 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, 91% of cyberattacks and their resulting data breaches now begin with a spear phishing email message.

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

We often associate phishing with cybercrimes that relate to online banking: 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.

**91%**
of cyberattacks begin with a spear phishing email

But phishing covers 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.

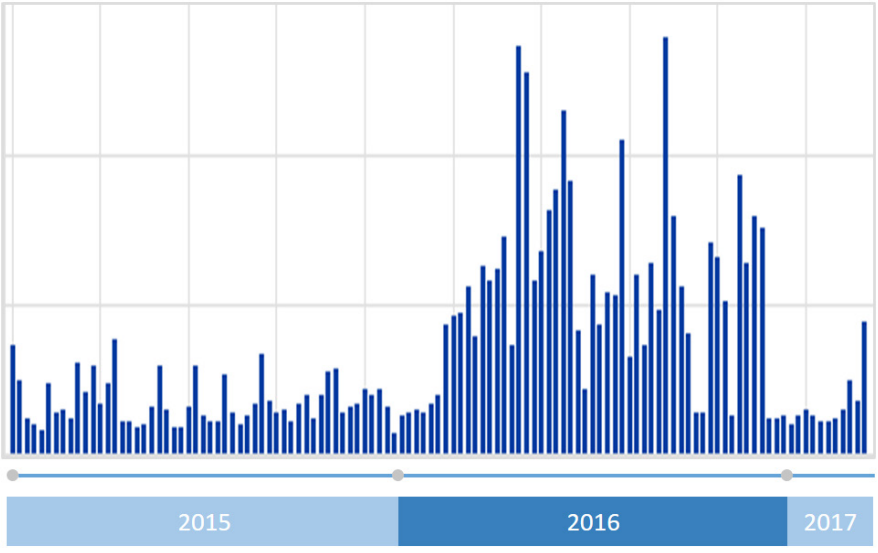
# Phishing is big business

In 2016, the volume of attacks increased dramatically, fueled 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 more savvy than they are. As such, 2016 has been dubbed the "year of ransomware".

Phishing campaigns are generally more successful when they use contextually relevant lures, and between 2013 and 2015, phishing attack trends followed consistent and predictable patterns. During each of these three years, phishing attacks tended to increase from month to month before finally surging in the fourth quarter of each year, during the holiday seasons.

However, this was not the case in 2016. Instead of peaking at the end of the year, phishing attack crested in the middle of the year with localized spikes in attacks that took advantage of regionally specific events or periods of fear and anxiety. For example, uncertainty around the United Kingdom Brexit vote was exploited to target government departments in May and June 2016. And tax return season in the United States saw IRS-themed attacks increase by 400% over previous years.

**Email threats 2015 - 2017**




In 2016, the volume of attacks increased dramatically, fueled by dark web services such as free phishing kits and phishing-as-a-service, it was dubbed the "year of ransomware".

# Improving efficiency and productivity

**89%**
of phishing attacks orchestrated by professional organized crime

For the most part, cybercriminals are interested in money. Either they'll extort money from you using ransomware or social engineering, or they'll steal data and credentials that can be sold via dark web markets. And as the phishing threat landscape evolves, so do the attackers.

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.

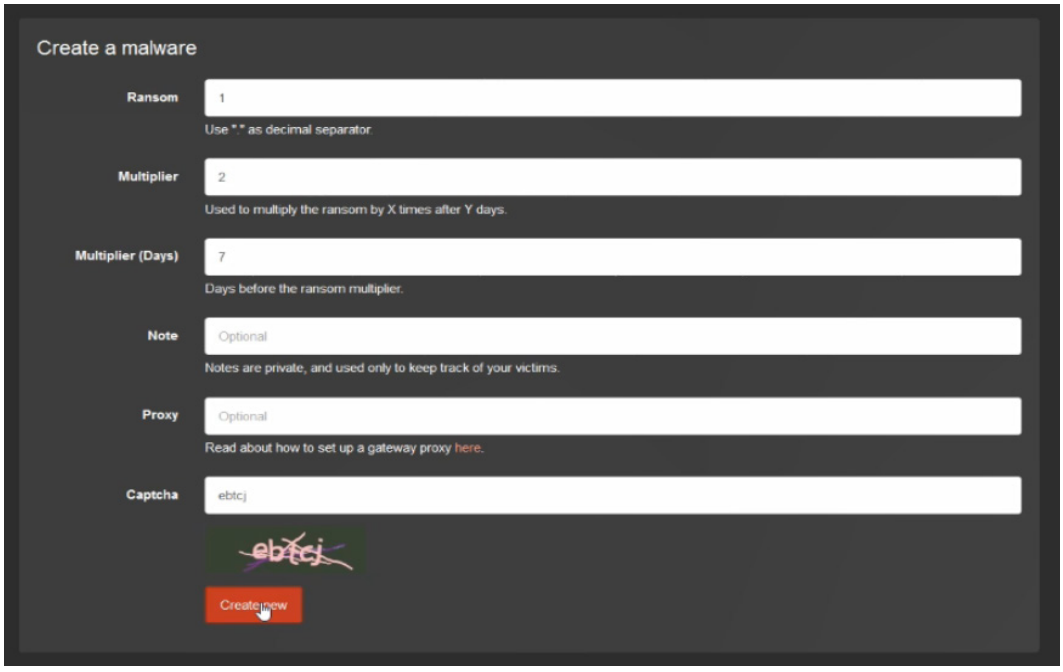
An interesting facet of the phishing ecosystem is that there are a large number of actors committing attacks, but only a small number of phishers that are sophisticated enough to write a phishing kit from scratch. Because of this, phishing kits are now widely available for download from dark web forums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

### Attacks-as-a-service

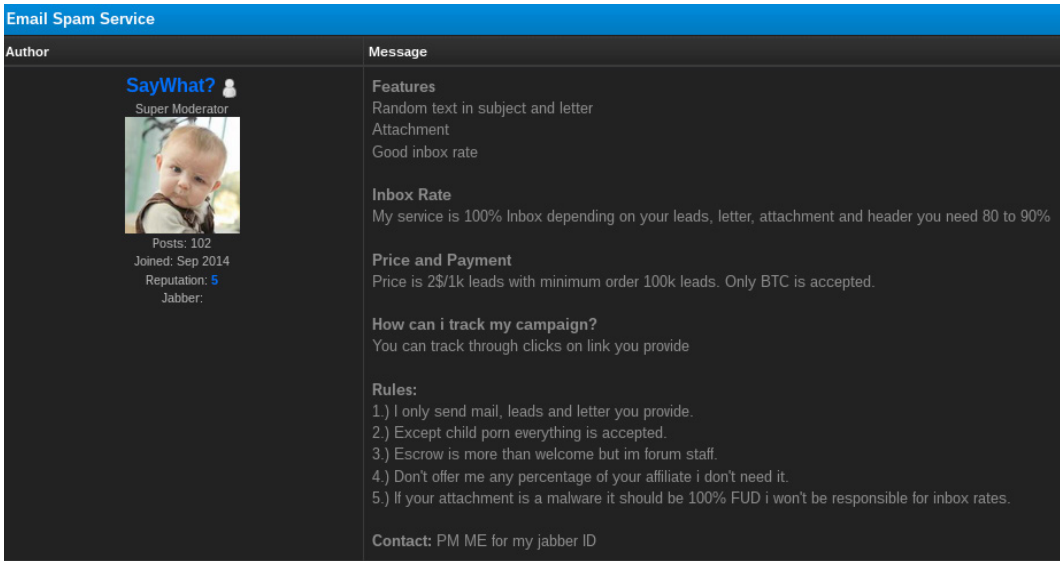
In fact, attackers don't even need to know how to create malware or send emails anymore. As-a-service and pay-as-you go solutions permeate most online service technologies, and phishing is no different – with a range of services increasingly available to attackers:

- **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.

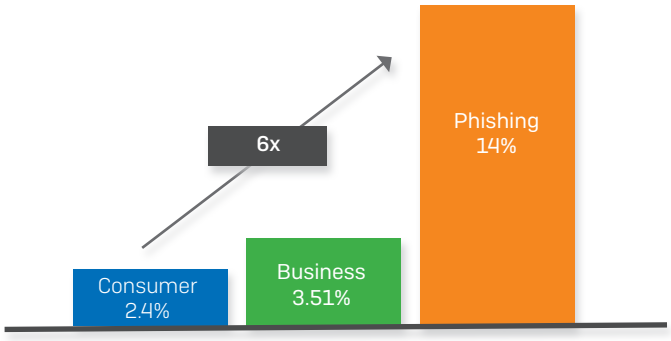
These services have led to the explosion of phishing attacks highlighted earlier, as any attacker can launch an attack regardless of technical skill.

### 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.

This newly-found research and development time has kicked phishing threats up a notch. We're now starting to see Business Email Compromise (BEC) attacks – a dangerous new subset of phishing attacks emerging that enable attackers to expand profit areas by targeting high value corporate targets.




Phishing email click through rates.

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

## 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 the recently emerging trend of Business Email Compromise tactic acting as a subset of spear phishing.

**$3.1 Billion**
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.

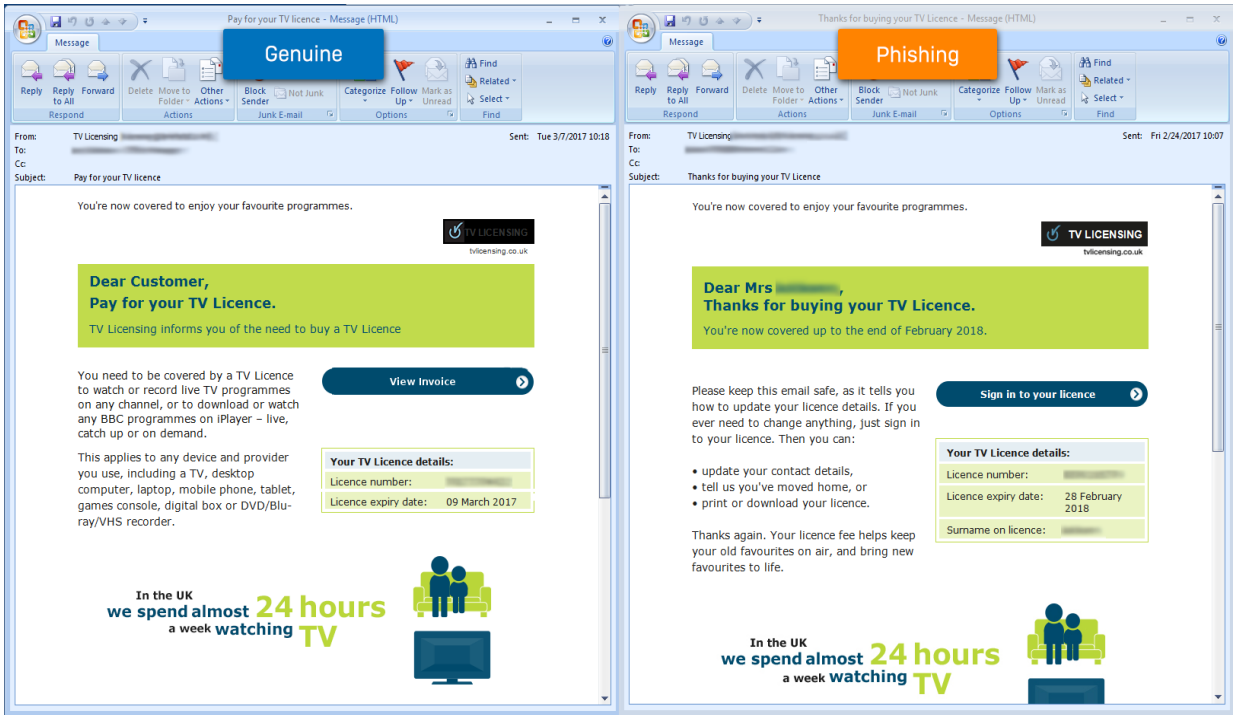
- Targeting the assets of individuals
- Typically consumers of a brand's products or services
- Impersonal batch and blast
- Focused on stealing personal data, such as login credentials


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.

Even more targeted subsets of spear phishing have since emerged using 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**

**$140,000**
Average loss per scam

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.

## Spot the signs

**30%**
of phishing emails are opened

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 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 emails come in all shapes and sizes, and unfortunately, no single product will fully protect your business from phishing attacks. A multi-layered defense against phishing attacks, combining advanced security technologies and educated, phish-aware employees, is the only answer.

**To be protected, you need multiple lines of defense:**

| Stop threats at the door | Protect your weakest link: Users | Secure your last line of defense |
|---|---|---|
| **Email and web protection** | **User training** | **Anti-exploit and anti-ransomware protection** |
| • Live threat updates<br>• Block malicious attachments, content and URLs<br>• Anti-spoofing<br>• URL filtering<br>• Time-of-click URL protection<br>• Malware sandboxing | • Training<br>• Testing<br>• Reporting | • Next-gen exploit prevention<br>• Analysis<br>• Clean up |
| **Sophos Email Protection**<br>**Sophos Web Protection** | **Sophos Phish Threat** | **Sophos Intercept X** |

### Stop threats at the door

Your first opportunity to defend against phishing attacks and other email-borne threats is strong email and web filtering.

The best defense against phishing emails is your email gateway. Email protection is your watch guard, blocking 99% of unwanted email at the gateway, including malicious attachments, content, and URLs - long before an end user ever sees them. Time-of-click technology stops your users from clicking through to infected websites – even if they were clean when the email entered your inbox – and cloud sandboxing detonates emails with macro-laden attachments far from the inbox.

Web filtering is another must-have as a front-line defense, filtering and blocking infected URLs should your users click an email link. And file sandboxing ensures those nasty malware laden downloads get removed from the threat chain early on.

### Protect your weakest link: users

Even with the best upfront filters, attacker methods such as BEC – with no executables or links to detect – may still get through. Appropriate training and education is critical for ensuring that all your employees know how to spot and deal with these types of email messages. Look for solutions with editable campaign simulations that can be made relevant to your organization, and those that allow you to report on employee performance in order to reward good performance and help improve others.

### Secure your last line of defense

If your click-happy end users inadvertently unleash potent, powerful malware onto your systems, there's still ample opportunity to stop the damage – and even reverse its effects. Next-generation exploit prevention solutions will identify, analyze, and neutralize the effects of even the most advanced, unseen malware out there, and automatically clean up all trace of infection so you can get on with your day.

### Know your business

Make sure your company processes are understood, that you encourage employees to question requests that seem out of character from other employees and senior managers (no matter how senior!), and perhaps most important of all, ensure you have a two-stage approval process for all significant fund transfer requests. All the defenses in the world aren't going to stop an employee from unknowingly sending large payments to a thief without some proper checks and balances in place.

Sophos has powerful technologies that can protect you at each stage of an attack. For more information visit Sophos.com/phishing.

# 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

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

Oxford, UK


2017-04-03 WP-UK (MP)