usecure

Your Complete Guide To **Employee Phishing Scams**

What Is Phishing?

Phishing is a form of fraud in which an online attacker, usually impersonating a trusted source, influences a victim to disclose sensitive information, or click a harmful link.

The motive of launching a phishing scam can range, although financial gain, data theft and even competitive advantage are often the cause.

How Does It Work?

Phishers use a range of tools to reach out to their victims, including text messages, social media and mobile phones are all options for an attacker, although email is undoubtedly the most popular weapon of choice.

Many of these scams are emailed in a “spray and pray” approach, with generic email templates sent out in their masses in the hope of tricking a number of unsuspecting users.

Social engineering and pretexting techniques offer much more personalised techniques of attack - with prior research of a victim being used in order to add some extra layers of knowledge and trust in the eyes of an unsuspecting victim.

Why Is Phishing So Successful?

- A lack of employee awareness training
- Increasingly sophisticated techniques
- More personalised campaigns
- The widespread availability of phishing tools

No awareness?
Big problem.

97%

The percentage of people around the world unable to identify a **sophisticated** phishing email

InspiredLearning, 2017

12%

The percentage of users who **click the link** after opening a malicious email.

Dashlane, 2018

The Most Common Types Of Employee Phishing

Email Phishing: The original.

This scam often relies heavily on a 'spray-and-pray' approach, where fraudulent emails are sent in their masses to a large number of recipients.

These emails often impersonate a known or trusted company or individual, with the aim of tricking a person into parting ways with personal information - whether that be login credentials or banking information. Attacks can also encourage an unsuspecting user to download a harmful email attachment or a file from a fake website - opening the door to a damaging malware infection.

All of this is made possible by what's known as 'email spoofing', where email headers and subject lines are forged to make the email look as legitimate as possible. Huge organisations such as Apple and Microsoft are often spoofed in these attacks, due to their huge number of users and trusted reputation.

Spear Phishing: Time to get personal.

Not all phishing scams are generic. 'Spear phishing' fraudsters customise their attack emails to contain the target's name, company, position, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender.

Spear phishing is especially popular on social media sites like LinkedIn, where attackers have a range of useful information.

Whaling: There's always a bigger phish.

In another scam involving the bigger fish of the organisation, a whaling attack targets only an organisation's top executives. The term whaling reflects exactly this - with a cyber criminal not wanting to waste time on smaller fish and, instead, targeting the 'whales' of the company due to the value of information they hold.

Prior research is also important for the criminal here, with social engineering techniques being deployed in order to obtain information that can later be used in the phishing email.

BEC/ CEO Fraud: The art of impersonation.

In this increasingly common phishing scam, attackers can compromise the email account of a high-level exec or financial officer via an already successful spear phishing attack, or previous infection. The criminal then patiently spies on the account's email activity, while gathering valuable information on processes and procedures of the business.

When equipped with enough information to effectively impersonate the executive, the attacker will send an email - usually containing urgency or high importance - and requests that the victim transfer funds to a specified account. Sure, it's a riskier scam, yet still a lucrative favourite in the world of cyber crime.

How To Spot The Red Flags Of A Phish

#1. Mismatched URLs:

Often, the embedded URL in a phishing message will appear to be perfectly valid, but when hovering your mouse over the URL, the actual hyperlinked address may appear differently. This is an indicator that the link could be fraudulent.

#2. Poor Spelling/ Grammar:

Large companies often have strict processes in place for reviewing company messages, especially when it comes to grammar, spelling and legality. So if you receive a message littered with mistakes, there's a chance it may not be from a legitimate source.

#3. Requesting Personal Info:

No matter how legitimate or official an email looks, it's always a suspicious sign when they ask you for personal information. Banks and reputable companies will never ask you to send account or credit card numbers, as they should already know these details.

Others To Look Out For:

- Special offers that sound too good to be true
- 'Responses' from companies you've never contacted
- URLs containing a misleading domain name
- Unrealistic threats, like having your account deleted
- Emails that contain attachments/ website links
- Messages that urge you to act quickly

Tricky subjects.
The Top 10.

The most common words in **BEC phishing** email subject lines.

Rank	Subject Line	%
#1	"payment"	13.8
#2	"urgent"	9.1
#3	"request"	6.7
#4	"attention"	6.1
#5	"important"	4.8
#6	"confidential"	2.0
#7	"immediate response"	1.9
#8	"transfer"	1.8
#9	"Important update"	1.7
#10	"attn"	1.5

The Main Targets In Your Business

The C-Suite:

A senior exec's access to sensitive information and authority to sign-off high-value transfers gives cyber criminals a host of incentives.

Phishing emails that target executives typically take the form of sensitive information requests from a legitimate-looking source. By creating a spoof email where a 'credible' sender appears, the attacker can make requests to executives that are far less likely to be denied.

...How To Protect Your Execs:

Make additional authentication or verification steps a requirement for any sensitive requests (such as wire transfers).

Also, encourage executives to limit both what they are sharing and who they are connecting with on social media.

Administrative Assistants:

Their role on the front line, combined with their privileged relationships, makes your admin team an attractive and accessible target.

Phishing emails targeting these assistants often come as a request from another executive, usually asking to review an attachment or to send across financial information. If the phishing attempt is successful, then eavesdropping software can be installed, meaning that the assistant's privileged information can be leaked.

...How To Protect Your Admins:

Provide them with a clear procedure for dealing with phishing emails and make sure that there is a good spam filter set up.

If the admin assistants come across a non-legitimate looking email, they should feel actively encouraged to report it to IT support and know exactly how to do so.

Human Resources:

HR professionals are often some of the most highly-connected people in any business. They regularly communicate with existing and potential employees - and phishers are waiting to take advantage of this.

Cyber criminals often pose as potential employees by sending malicious payloads disguised as CVs, or will even impersonate a high-level exec and ask for information regarding personnel. The tax season is especially full of phishing attempts on HR, with employee tax information being a big target.

...How To Protect Your HR:

By investing in benefits software and employee portals, you can reduce the number of confidential documents that employees send via email. Requests from an employee asking for sensitive information should be verified either face-to-face or over the phone.

Sales/ Business Development Managers:

Business development managers, account managers, and internal salespeople constantly interact with prospective and existing clients. In person, over the phone, or via email, they're eager for emails from potential customers and want to be as responsive as possible.

An attacker can easily locate their name, phone number, and email address online, and the chances of the message being opened are high. Stealing credentials from these salespeople can provide access to customer lists, pricing sheets, and confidential deal information.

...How To Protect Your Sales Team:

Consider email-alternative methods with your purchasing department on how to transfer invoices.

Ensure that your sales team are encouraged to double-check any linked-text they receive in emails.

Random Employees:

The inconvenient truth is that anyone in your organisation can be targeted by a phishing attack. Awareness programs , mock phishing exercises, and security measures need to be addressed with everyone in the business, no matter what position or level they may be at.

The more that employees are involved in security efforts, the stronger your security level will be.

...How To Protect Your Workforce:

Ensure that company-wide security awareness training is in place for ALL users, regardless of what level or department an employee is at.

How To Raise Employee Phishing Awareness

Raise awareness.
Mitigate the threats.

#1 Phishing Awareness Training

What is employee phishing awareness training?

Employee phishing awareness training is exactly what you'd think it is -- enlightening your users on how to spot, avoid and report a suspected phishing attack.

For years, this type of training fell into the once-per-year tick box exercise in front of a room of employees suffering in the midst of a 'death by PowerPoint" presentation.

Thankfully, this type of training is now deemed as ineffective and has been replaced by modern eLearn-inspired courses.

How does it work?

As phishing is just one threat in a never-ending line of attacks, these types of courses often fall into a security awareness programme that covers a variety of threats.

These courses are usually delivered online, where training can be completed at a time of the users choice and progress can be made without your IT team running the unbearable task of controlling every aspect of your programme.

How does it work?

Many organisations begin by looking at how they can create, implement and maintain their security awareness training in-house. The problem is, creating an in-house programme can often sound complicated, expensive and pretty daunting. Truth be told, that's because it is.

We suggest you start off by researching the different third-party training solutions out there on the market, rather than inflicting the headache-prone task of lumbering this responsibility onto your IT team (which they'll thank you for later).

What phishing awareness **should** be:

- Short and engaging
- Regularly delivered
- Progression tracked
- Relevant to modern day

What phishing awareness **shouldn't** be:

- Sporadically delivered
- Measure by tick boxes
- PowerPoint-driven
- A one 'size fits all' approach

70%

The percentage of risk **reduced** by investing in training.

AberdeenGroup, 2016

#2 Phishing Your Own Users

What is simulated phishing?

Simulated phishing tests have become a go-to method for IT professionals when determining just how vulnerable your employees are to an inevitable real-world attack.

With these mock exercises, you're able to launch a phishing 'attack' on your employees in order to determine how susceptible your users would be to the real thing.

What the benefit of phishing my users?

With these tests, you're able to clearly visualise the opened, clicked and compromised rates of your employees - giving you a key insight into the susceptibility level of your users.

Here's a breakdown of what else your simulation can achieve:

- Clearly assess user vulnerability
- Give users real-world experience of an attack
- Determine where education is most needed
- Demonstrate the need for security training budget

How does it work?

The easiest way of launching a phishing simulation test is by utilising the tools already out there. You can try our uPhish simulation tool for free at www.getusecure.com, or, take advantage of our phishing managed service.

Simulated phishing **in action.**

-23%

The average decrease of users who **visit** the login page during a second phishing simulation.

usecure (phishing results), 2018

-17%

The average decrease of users who give away **account credentials** during a second phishing simulation.

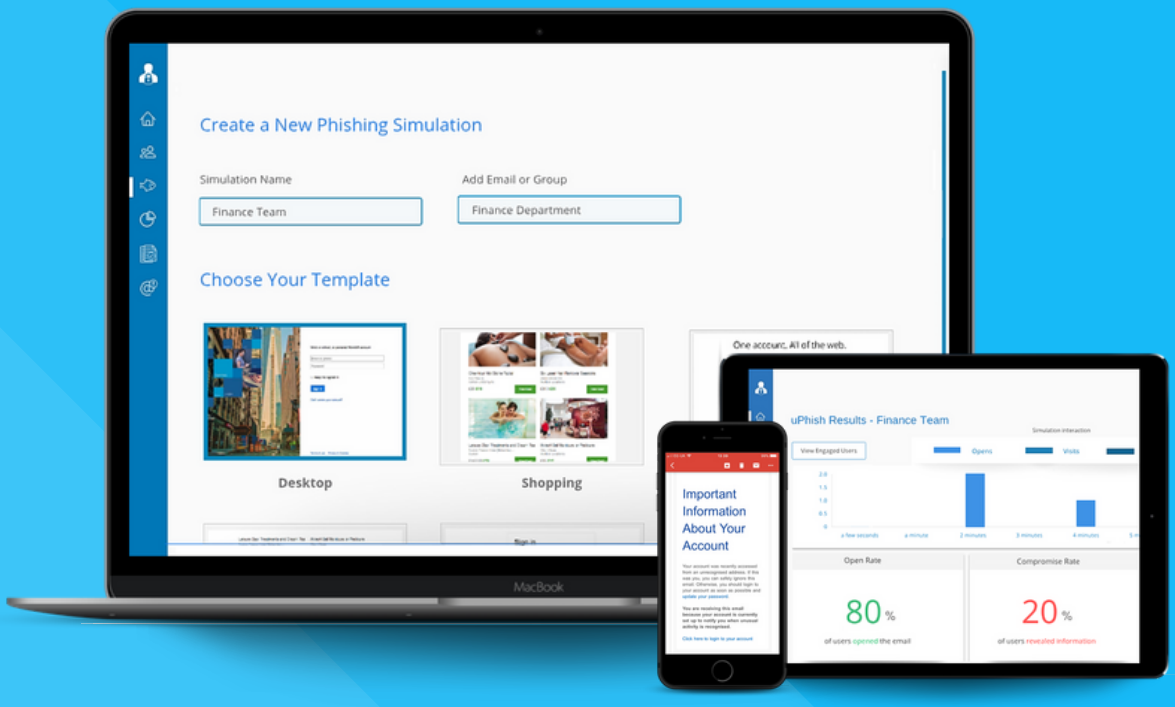
usecure (phishing results), 2018

usecure

Launch Your Free Simulated Phishing Test

Determine how vulnerable your users are to a real-world phishing scam.
Visit www.getusecure.com, or, get started below.

Get Started



T: 0161 214 0869 **E**: info@getusecure.com **W**: www.getusecure.com