Phishing Attacks:

A Cyber-security Guide for Employers and Individuals

Table of Contents

Introduction

With every cyber-attack, it becomes increasingly clear that no one is safe from data breaches or cyber-extortion. Whether you are an employer that stores proprietary data or an individual with financial and personal information at risk, hackers won't rest until they have what's yours. And their tactics continue to evolve.

Cyber-criminals have a variety of tools and techniques at their disposal, including malware, ransomware and disrupted denial-of-service attacks. One of the most common and difficult-to-spot strategies hackers use is phishing scams, which require minimal technical know-how and can be deployed from anywhere in the world via a simple email.

In broad terms, phishing is a method that cyber-criminals use to gather personal information. In these scams, phishers send an email or direct users to fraudulent websites, asking victims to provide sensitive information. These emails and websites are designed to look legitimate and trick individuals into providing credit card numbers, account numbers, passwords, usernames or other sensitive information.

> Recent research revealed nearly 40% of UK organisations experienced a phishing attack in the past year.

With every opened email, users risk becoming the victim of monetary loss, credit card fraud and identity theft. What's more, successful phishing attacks oftentimes go unnoticed, which increases the risk of large and continued losses, particularly for businesses.

Even in the face of highly funded cyber-security measures, phishing scams can be financially devastating. In 2017, tech giants Facebook and Google were phished for over £76 million each, proving that protection from online scammers doesn't come easy—even for large-scale companies.

What's more, under the General Data Protection Regulation (GDPR), UK organisations are required to implement strict data protection policies for both their customers and employees, or otherwise run the risk of a potential data breach and hefty government fines. In terms of phishing, the GDPR requires organisations use protective measures such as pseudonymisation and encryption to decrease the risk of phishers getting access to sensitive data.

Phishing is becoming more sophisticated by the day, and it's more important than ever to understand the different types of attacks, how to identify them and preventive measures you can implement to keep yourself safe.

This guide provides readers with a variety of sample phishing emails, which can help you better identify and delete dangerous messages before they do irreversible damage. In addition, you will learn about the common strategies that phishers use to steal your data and ways to keep yourself safe.

Phishing versus Spear Phishing

Often, the terms phishing and spear phishing are used interchangeably. However, there is a key distinction between these two types of attacks, and it's important to have some basic background knowledge.

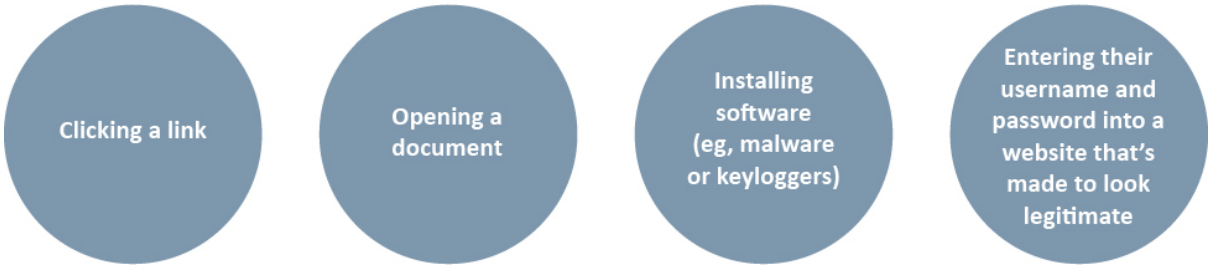
According to a report from the Ponemon Institute, human error accounted for nearly 30% of worldwide data breaches.

Phishing

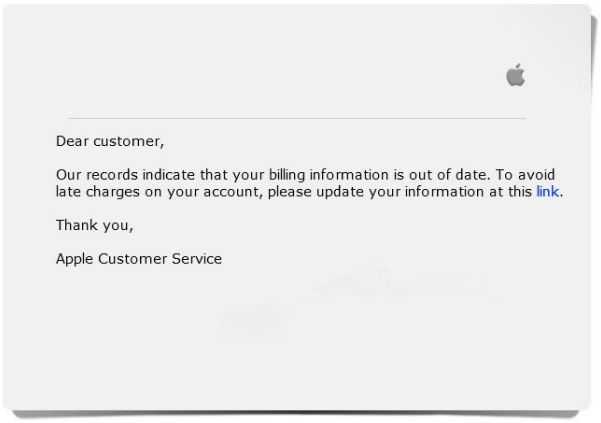
Phishing is a general term that refers to any cyber-attack where a hacker disguises themselves as a trusted source in order to acquire sensitive information. Typically, under traditional phishing attacks, hackers send fraudulent, malicious emails to as many people as possible. It's not unusual for phishing attacks to target thousands of individuals at once in the hopes of netting just a few victims.

Phishing attacks take a quantity over quality approach. Despite the randomness of the attacks, phishers can gain highly sought information on their victims through mass, easy-to-reproduce emails. The goal of these emails is to compromise data or a larger network through the greatest cyber-security vulnerability of all—users themselves. Effectively, instead of going through the hassle of breaking strong, digital defences, hackers use phishing attacks to trick someone into giving them access to a network or data.

To fool the victims, attackers customise phishing emails to make them appear legitimate, sometimes using logos or dummy email accounts to improve the effectiveness of the attack. Usually, phishers will pretend to be a trusted source, like a hospital, bank or employer. The phishing message will likely include alarming or suggestive language to fool victims into:



If a victim does any of the above, the hacker can infect their computer and steal sensitive information, often without having to use a single line of code. With phishing attacks, even the most top-of-the-line firewall can't stop an individual from clicking on a malware-loaded email. And, once a single computer gets infected, the malware can spread throughout an entire network.



Dear customer,

Our records indicate that your billing information is out of date. To avoid late charges on your account, please update your information at this link.

Thank you,

Apple Customer Service

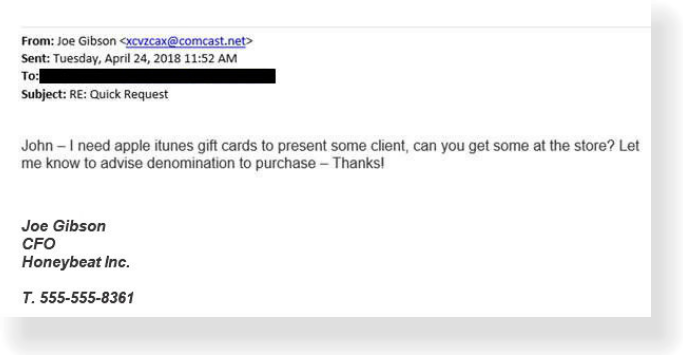
To the left is a sample of a phishing email. In this example, the phisher is impersonating a popular company (Apple) in order to trick you into clicking a link. This link could redirect you to a fraudulent website to either steal your personal information or install malicious software on your device.

Spear Phishing

While phishing attacks are effective, they are designed to be broad and affect as many individuals as possible. As a result, they are generally written vaguely and are easy to spot. Spear-phishing attacks are much more convincing, targeted and sophisticated.

With spear phishing, cyber-criminals narrow down the scope of their attack to a smaller group, sometimes just a handful of individuals. By doing this, hackers can do research and make the phishing email much more convincing based on a victim's profile or online activity. Malicious hackers can find most of the information needed to carry out a spear-phishing attack right on the internet, particularly on company websites and social networking sites. It's not uncommon for phishers to use a target's personal information (eg, name or address) or the personal information of their friends, family and colleagues as leverage in an email.

Because spear-phishing attacks are highly customised, they are far more likely to succeed than traditional phishing attacks. What's more, spear-phishing attacks often have specific goals. For instance, a phisher may target certain individuals based on whom they work for, the type of information they have access to or their financial status. Spear-phishing attacks may focus on a particular company, organisation, group or government agency based on the potential ROI.



From: Joe Gibson <xcvzcax@comcast.net>
Sent: Tuesday, April 24, 2018 11:52 AM
To: [redacted]
Subject: RE: Quick Request

John – I need apple itunes gift cards to present some client, can you get some at the store? Let me know to advise denomination to purchase – Thanks!

Joe Gibson
CFO
Honeybeat Inc.

T. 555-555-8361

To the left is a sample of a spear-phishing email. In this example, the phisher is impersonating an executive of a company and asking an employee to complete an urgent task for them. Here, the phisher is hoping to trick the user into replying to the email, which could help the cyber-criminal steal or gather sensitive information.

The Targets

Both phishing and spear-phishing scams can affect anyone. Phishing attacks are more expansive and don't necessarily have a psychology behind who is attacked. Spear-phishing attacks, however, are more thought out and planned. These attacks often have one of two targets: individuals or employers.

Individuals

Cyber-criminals target individuals because they are the easiest to compromise and the most susceptible to phishing attacks. This is because many people aren't tech-savvy or educated on how to spot phishing emails.

In addition, individuals are attractive to hackers because they usually have a credit card or bank account. Phishers can gain a variety of sensitive information from an individual, including banking information, eBay, Facebook, PayPal and Venmo credentials. With this data in hand, cyber-criminals can steal money or even identities with ease.

Employers

For employers, every one of their employees represents a potential exposure to phishing attacks. In fact, a skilled scammer could easily trick employees at every level of the organisation. This puts a company's financial information, trade secrets, confidential documents and network at risk.

Employers are often the target of highly focused spear-phishing campaigns as well. Using names and contact information easily retrieved from company websites, cyber-attackers create convincing emails to fool employees. In these attacks, scammers use job responsibilities, company details and co-workers' names to lure users into spear-phishing attempts, giving hackers all they need to access company systems. Executives are not exempt either and might actually be easier targets, as their information is more widely available to the public on social media sites and company websites.

Targets of these attacks will typically vary based on a phisher's motives and the type of data they're after. While financial gain is often the primary driver for phishing attacks, stealing internal corporate data, leaking trade secrets or committing corporate espionage are also common goals.

Employers of all sizes and industries are at risk; however, online payment services, internet-based financial businesses and retail sites are among the most targeted sectors.

What's at Risk?

Of all the various types of cyber-crime, phishing attacks are some of the most dangerous. This is because phishing messages can easily bypass standard antivirus software and pass through spam filters. What's more, scammers don't need to infect your computer with a virus to obtain your information. Instead, criminals rely on psychology and misdirection.

Simply by clicking links, replying to an email or completing forms found in fraudulent emails, you give hackers all the information they need.

Following a phishing attack, employers and individuals could lose any of the following information:

- **Login credentials**
- **Banking credentials**
- **Credit and debit card information**
- **Addresses and other personal information**
- **Trade secrets**
- **Confidential documents**
- **Medical information**

For businesses, the risks of phishing are magnified. This is because, by infecting a single user, hackers can launch even more penetrating attacks on an organisation's network, stealing credentials, disrupting critical processes, or encrypting data and making it impossible to access.

How Cyber-criminals Plan Their Attacks

While the content of phishing and spear-phishing emails can vary, cyber-criminals often employ similar strategies and tactics. Using these methods, phishers have proven repeatedly that they can affect users regardless of their position in companies, presumed level of technical expertise or employment field.

What's more, targets are not always key employees in a business—anybody can be a victim. To avoid becoming prey to a phishing scam, it's important to understand how cyber-criminals think when creating and sending phishing emails. When carrying out a phishing attack, hackers will generally follow four basic steps:

1. **Target identification**—When identifying targets, phishers may create master email lists. These lists will either consist of random email addresses for larger phishing schemes or more focused targets for spear-phishing attacks. If the phisher is after a particular business, they might concentrate on executives or high-level managers with greater levels of access. In other cases, phishers may target lower-level employees who may respond to pressure from someone impersonating their boss. In most cases, the targets of more tailored spear-phishing attacks are those that have valuable information or the authority to transfer funds.

2. **Intelligence gathering**—With a target in mind, in the case of spear-phishing attacks, the phisher's next job is to search social media, company websites and the dark web for enough information to build a believable email. These emails may include personal details, professional affiliations, or the names of acquaintances and family members. Phishers have also been known to collaborate with other cyber-criminals, trading victim emails and vital information to enhance the effectiveness of an attack.

    - The level of intelligence gathering will depend largely on whether or not the attacker is deploying a spear-phishing or broader phishing attack. The larger the scope of an attack, the less specific the phishing email will be. Conversely, the more valuable the information, the more planning and research the criminals have to do. For example, a phisher looking to steal trade secrets from a specific company will have to conduct more research than if they were simply trying to steal login credentials from any individual.

3. **Message crafting—**Using all the information gathered, the phisher will craft the most convincing email possible. Scammers may insert logos of popular websites (eg, PayPal, Amazon or eBay) and official-sounding verbiage in their own malicious email template. Typically, phishers will ask for your username and password in the body copy of the email. The email will be worded with a sense of urgency so the end user feels like they will lose the account or money if they don't comply immediately. The goal of hyper-targeted spear-phishing emails is the same as any other phishing attempt—get the user to take an action that will benefit the scammer.

4. **Email deployment—**While spam filters and other solutions can prevent phishing emails from affecting employers and individuals, no tool is 100 per cent effective. In fact, all a phisher needs to do to ensure an email is delivered is to trick email filters into thinking a message was sent from a legitimate source. One way they do this is through display name spoofing, a method where an email's 'From:' field is made to look like a safe source. Frequently, attackers will register a free email account and, in the case of spear-phishing attacks, will use specific names or companies the victim will recognise.

Attack Strategies

The effectiveness of a phishing attack is limited only by the sender's imagination. Again, the content of these attacks may differ depending on the scope of the scam, but most use a combination of the following strategies.

Impersonation

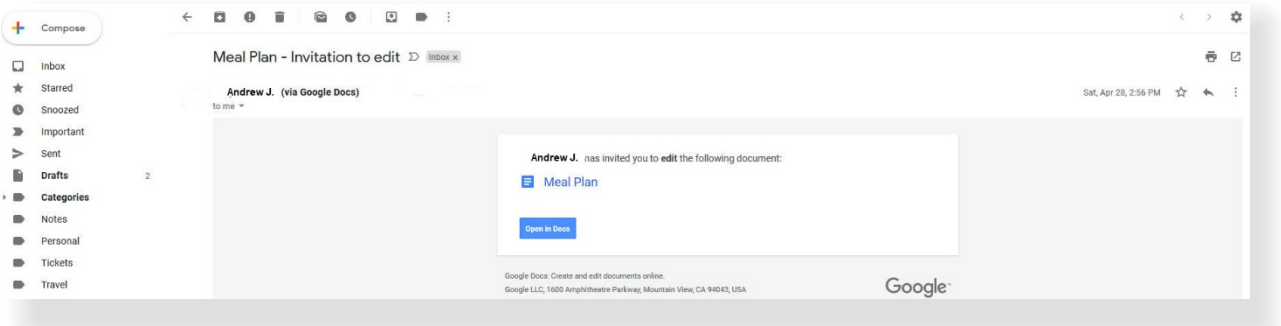
A common tactic for spear phishers is to impersonate someone the victim knows, like a co-worker, friend or family member. Attackers may pretend to be a high-level executive asking an employee for sensitive information and credentials. Attackers may also impersonate loved ones and ask an individual to wire money following an alleged emergency.

When it comes to spear-phishing emails, you can't assume that personalised messages indicate a legitimate email. In fact, in finely crafted spear-phishing scams, the attacker will have done their research and may include specific names, dates and details the user is familiar with and likely to respond to.

Impersonation is part of a larger strategy cyber-criminals use called social engineering. Social engineering is the art of accessing information, physical places, systems, data, property or money by using psychological methods, rather than technical methods or brute force. These attacks can occur in a number of different forms, including a well-crafted spear-phishing campaign, a plausible-sounding phone call from a criminal posing as a vendor or even an on-site visit from a 'fire inspector' who demands access to a company's server room.

Real-life Example

In May 2017, work halted for 3 million people when phishers were caught sending fraudulent invitations to edit Google Docs. When opening the invitation, people were brought to a malicious third-party app, which allowed the hackers to access people's Gmail accounts.



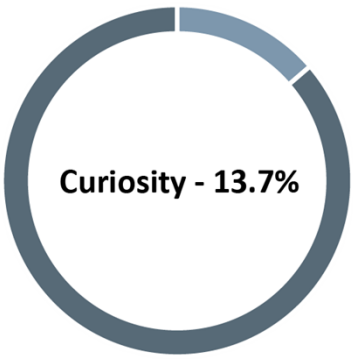
In the above example, cyber-criminals are posing as a friend or family member. In doing so, they hope to trick victims into clicking on a fraudulent link to a Google Doc and providing sensitive information. As you can see, phishing emails can be quite convincing when put together by creative scammers.

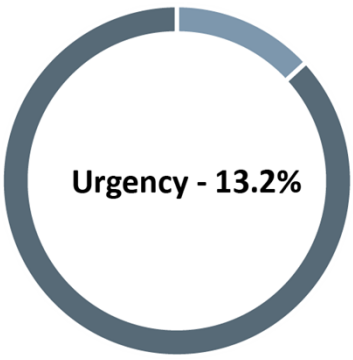
Fake President Fraud

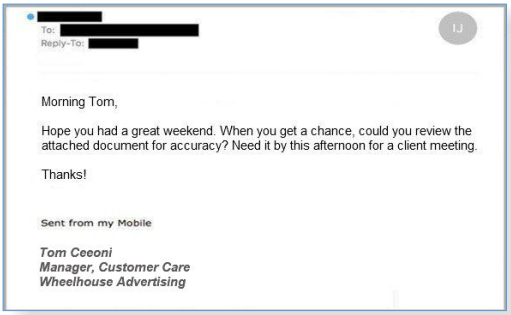
One subset of impersonation and social engineering is commonly referred to as fake president fraud. The fake president fraud is a type of scam in which a criminal posing as a company executive convinces an employee to voluntarily transfer a large sum of money directly to a criminal's account. The fake president fraud may vary in some of its details, but it always contains four major elements:

1. **The 'president' makes contact.** Someone posing as a high-level executive in the company—often the president, CEO or CFO—will reach out to the target employee. This contact often occurs via email, either from a domain that is deceptively similar to the company's actual domain or via a 'personal account'.
2. **The 'president' asks for a wire transfer.** The 'president' asks the employee to wire a large sum of money to a foreign bank account. The employee might be told that the money is for a host of seemingly legitimate purposes (recent acquisitions, paying off debts, paying vendors, etc.).
3. **The 'president' pressures compliance.** At this point, many employees may question the unusual request or the break in typical company protocol. That's when the 'president' deploys psychological pressure on the employee to accept the scenario as genuine and comply with the request. Those pressures can rely on a number of different factors, including the following:
    a. **Authority**—The criminal will emphasise their rank to convince the employee. This offers the criminal many options, such as using that authority to intimidate the employee or preying upon the employee's desires to impress a superior.
    b. **Time pressure**—Criminals will often claim that the transfer is an urgent matter, forcing the employee to ignore typical protocol and eliminate the chance that they might disclose the transfer to another party or verify the information before making the transfer.
    c. **Secrecy**—Often deployed in conjunction with time pressure, the 'president' may emphasise that this deal must remain secret for strategic or legal reasons. Having the employee 'in' on the secret can make them feel special and thereby increase the chance that the transfer will go through.
4. **The employee makes the transfer.** The employee contacts the bank, and the bank then makes the transfer. Even if it is unusual, the bank will transfer the funds to the account if the employee making the request is authorised to do so.

According to a report from PhishMe, the top reasons people are duped by phishing emails are:







In the example to the left, a cyber-criminal posing as a manager or executive is attempting to trick an employee into opening a malicious attachment. These types of phishing emails are some of the most common, as individuals are less likely to question something if they are faced with an urgent request from a peer.

Whaling

Whaling is another example of an impersonation scheme. However, in whaling attacks, cyber-criminals specifically target high-profile business executives. These emails are sent to a single person or small group of targets, which differs from the mass distribution techniques used in standard phishing attacks.

In these scams, the fraudulent emails and webpages are designed to appear like a critical business email from someone with legitimate authority, either externally or internally. Whaling falls under the umbrella of spear-phishing attacks, as these emails usually address executives by full name, company and job title.

In whaling attacks, criminals are usually after confidential company information. This could be passwords to sensitive accounts or information on specific processes and products. Whaling messages often employ scare tactics, threatening legal fees, termination and bankruptcy to trick the victim into taking a specific action (e.g., clicking a link, downloading malicious software or completing a fraudulent form). The whaling email or website may come in the form of a false subpoena, a fake message from the police or some sort of critical legal complaint.

In this example, a cyber-criminal is posing as the National Cyber Security Centre—a well-known organisation. This whaling message is designed to appeal to executives through specific, meaningful copy and a design that is well-above the standards of the average phishing email. The email prompts readers to download a maintenance update that will likely infect the company's entire network.

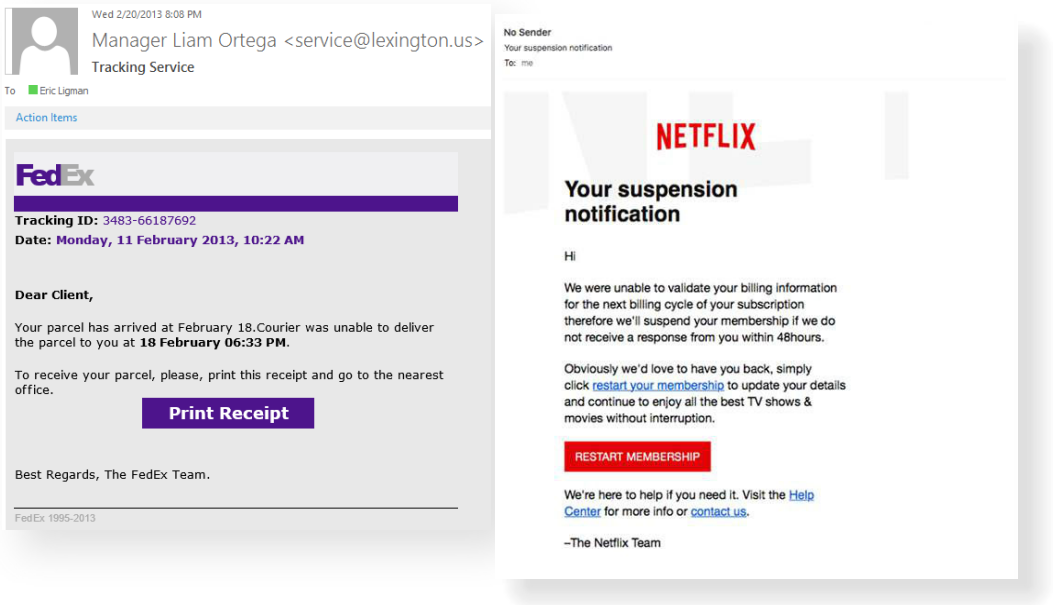
Urgent Requests

Phishers aren't afraid to use psychology to their advantage. These criminals know that impersonating an individual or organisation and urging immediate action can be incredibly persuasive. Often, these types of attacks threaten loss, punishment or added risk.

People are more likely to respond to phishing attempts if emails appear to be pressing or if the victim believes they are in some sort of trouble. Common examples of this type of fakery include, but are not limited to, messages from angry bosses, late credit notices, cancelled memberships, compromised accounts, missed parcel deliveries and missing rent cheques.

Emails like these may also appear as unsolicited requests to confirm account information or unexpected password reset requests, sometimes using your name in the body copy for added validity. The verbiage of these messages is often stern and will attempt to persuade victims to open attachments or reveal sensitive information.

When you get emails like these, it's a good idea to follow up with the sender using a method other than email. For emails from companies, you should call the customer service number listed on an organisation's official website. During your conversation, ask if you were meant to receive the initial email.



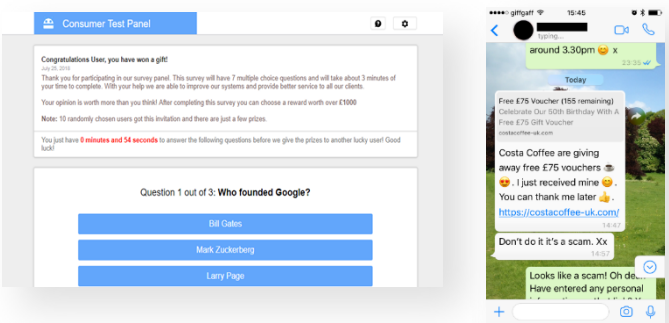
In the above examples, cyber-criminals are impersonating FedEx and Netflix. The use of branded logos and clean fonts make the emails appear more legitimate. Users are less likely to question emails if they look professional, so it's important to avoid clicking any links in an email unless you are 100 per cent sure they are genuine.

Unexpected Refunds, Payments and Contests

The allure of free money and gifts is difficult to resist, and phishers know this. It is not uncommon for phishing emails to bait victims with the promise of refunds, bank account adjustments or tax refunds. In broader phishing attacks, spammers may even claim you have won or are eligible for a contest or prize. Unsolicited emails of this kind are usually a dead giveaway for phishing schemes.

In 2018, cyber-criminals used WhatsApp, a cross-platform messaging service, to send spam emails offering free monetary vouchers for Costa Coffee. These messages promised a £75 voucher in celebration of Costa Coffee's 50th birthday, requesting users to click on the accompanied link and enter their personal information to claim their 'prize'.

A good rule of thumb to keep in mind to avoid becoming the victim of these kinds of scams is to think before you respond. Chances are if you receive a message relating to a contest you didn't sign up for or money transfers that seem out of place, the messages are fake.



In the examples to the left, cyber-criminals are using the allure of free money and gifts in an attempt to get users to click malicious links. Legitimate companies will rarely ask you to enter personal information through a suspicious link or survey for a voucher, discount or refund.

Vishing

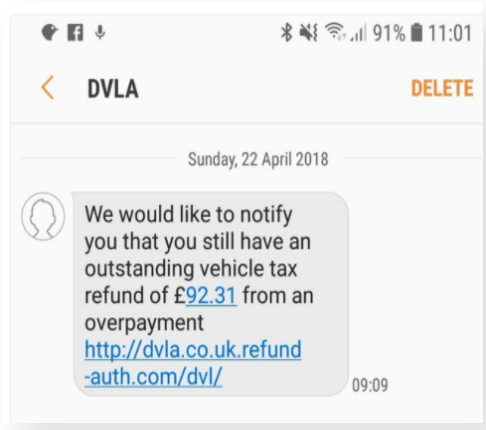
Vishing is a form of phishing that uses phone systems and similar technologies. Users may receive an email, phone message or text (usually called smishing) that encourages them to call a phone number to correct some discrepancy.

Typically, attackers use a technique called caller ID spoofing to make the calls appear like they are coming from a legitimate phone number. If a victim calls a number in a vishing scam, an automated recording prompts them to provide detailed information, including credit card numbers, birthdates and addresses.

A pair of Romanian hackers were recently charged with scamming victims out of £13 million in an elaborate vishing and smishing scam. To carry out the scam, the hackers installed interactive voice response (IVR) software on remote computers. These computers then initiated thousands of automated telephone calls and text messages.

The calls and messages appeared to come from a reputable financial institution, instructing victims to call a telephone number due to an account problem. When the victim called the number, they were prompted by the IVR software to enter their bank account numbers, PINs and other personal information.

To avoid falling for a vishing scam, never click links in a text message or respond to automated phone calls. Unless you were the one who initiated the call with a trusted source (eg, calling a known customer service number or reaching out to a bank using the number listed on their website), you should never share personal information over the phone. If you ever feel uncomfortable with the questions someone is asking you over the phone, tell them. If it's a genuine company, they should be able to provide different methods for contacting them, including setting up an in-person meeting at a legitimate place of business.



Smishing is a newer tactic employed by cyber-criminals. In principle, smishing scams have the same goal as phishing emails: get users to click a fraudulent link in order to steal information. In this example, a user was sent a malicious text, supposedly from the Driver Vehicle Licence Agency (DVLA).

How Your Data Gets Compromised

While most phishing attacks are sent by way of email or deceptive websites, cyber-criminals can take many other approaches. The following are just some tactics attackers use to steal your data and sensitive information.

High-profile Attack

The £150 million Facebook and Google attack—A hacker used a phishing email to trick Facebook and Google employees into wiring money to overseas bank accounts. Through this method, the hacker was able to net about £76 million from both companies.

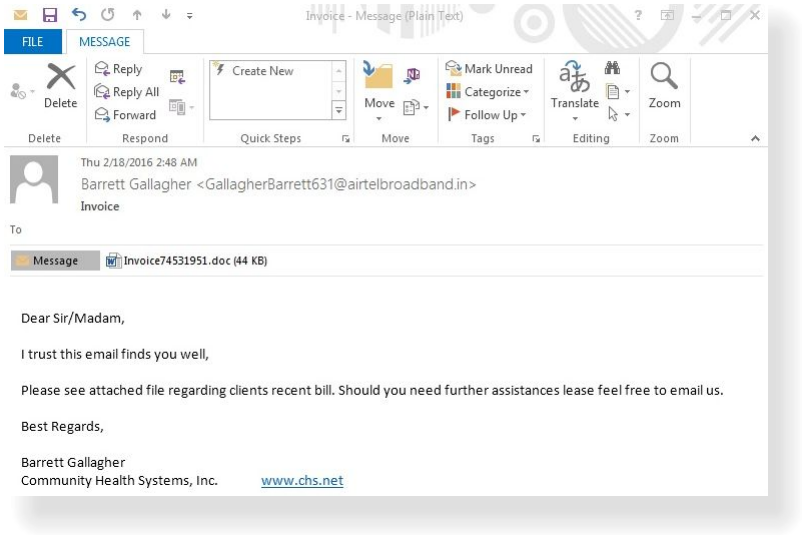
- Deceptive phishing—Deceptive phishing is the most common form of phishing. Under this type of scam, the attacker impersonates real companies in an attempt to steal your personal information or login credentials. Links in these phishing emails redirect users to a fraudulent website that has a nearly identical URL to its legitimate counterpart. Only a few characters will be out of order, making the phony links difficult to identify.

The example to the left highlights the convincingness of deceptive phishing attacks. Unless the user has the sense to look at the "From:" field (in this case, verification@GoDaddy.com), they may not know the email is fraudulent. In some cases, the "From:" field is so close to the legitimate counterpart that phony emails are difficult to spot.

High-profile Attack

Chipotle attack—A cyber-criminal group sent malware-laden emails to Chipotle staff. After employees opened the emails, the hackers compromised the point-of-sale systems of most Chipotle locations, using the breach to obtain credit card data from millions of people.

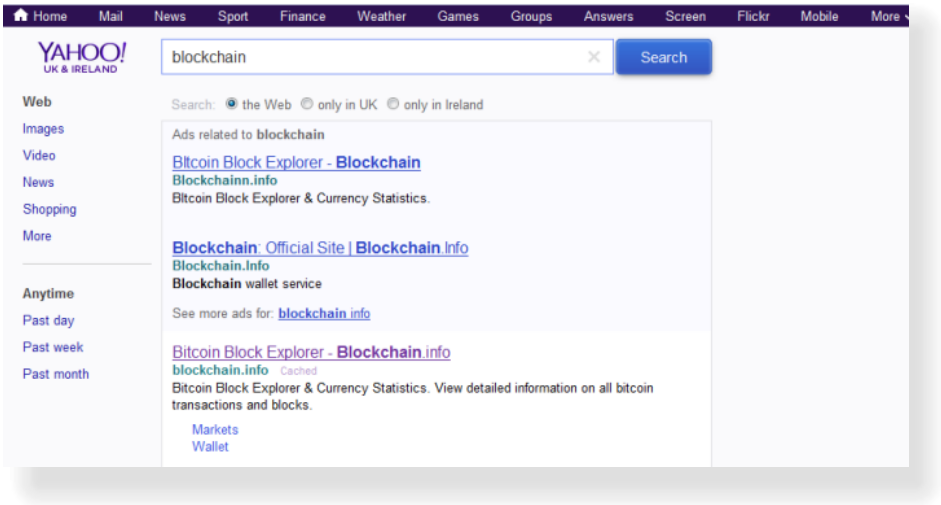
- **Malware-based phishing**—In order to steal your information, attackers will introduce malware—software designed to damage or disable computers—to a victim's PC. This is usually accomplished through email attachments or downloadable files from a website. In fact, email is commonly cited as the top method that hackers deliver malware to a user's computer. This strategy is often targeted at small and medium-sized businesses, as they frequently have lax cyber-security measures and perform sporadic system updates. Using these methods, hackers can introduce various malware into a network, including:
    - **Ransomware**—Ransomware is an increasingly popular style of malware. Using ransomware attacks, a victim's data is encrypted until a steep fee is paid. While pound amounts may vary, some ransomware attacks can cost six figures or more.
    - **Keyloggers and screenloggers**—Two common varieties of malware are keyloggers and screenloggers. In simple terms, these forms of malware track keyboard strokes of victims and relay the information back to the phisher. Advanced versions of these kinds of malware run automatically in the background and launch whenever a browser is opened.



One of the easiest ways phishers steal your data is through fake attachments. These attachments can carry hosts of malware or other malicious software—software that can monitor all of your activities without you even knowing it.

- **Session hijacking**—In plain terms, computer sessions are temporary interactions users have with websites. For instance, from the time you log in to an account (e.g., Facebook, Twitter or an online bank) until you log out is considered a session. Session hijacking occurs when malicious software 'hijacks' a user-initiated session. Phishers execute these attacks using local malware on a user's computer. Once deployed, session hijacking can be used to monitor all forms of online activity.

- **Pharming**—Pharming doesn't require an attacker to send thousands of emails and is effectively phishing without the bait. Pharming redirects a user's website traffic to another, bogus website using malicious code such as viruses, worms, Trojans and spyware. Even savvy users are often unaware that the website they are visiting is controlled by hackers.
    - One of the most deceitful methods of pharming involves web Trojans—malicious programs that collect a user's login credentials, using specific websites as a disguise. Commonly spoofed sites include social media platforms, company portals and email accounts. These fraudulent websites are designed to appear legitimate, when in reality victims are willingly handing their personal information to cyber-criminals. System reconfiguration attacks, tab-nabbing, DNS-based phishing and hosts file poisoning are other variations of this kind of attack.
- **Man-in-the-middle phishing**—Of all the varieties of phishing attacks, man-in-the-middle attacks are one of the hardest to detect. In these attacks, hackers position themselves between a user and a legitimate website, stealthily recording information. What makes them so hard to spot is that, during these attacks, a user's transactions and web activity are not visibly affected.
- **Search engine phishing**—Search engine phishing occurs when phishers create phony websites with too-good-to-be-true offers and index them within popular search engines. These scams are easy to fall for, as they appear during a user's usual internet usage. A common example of this is when phishers set up fake banking sites offering lower interest rates. A user would see this website appear in their search results and could easily be enticed into clicking the link and giving up their personal details.



Instinctively, users are apt to trust websites that appear at the top of search engine queries. Unfortunately, this is where many search engine phishing scams appear, so it's important to pay close attention to URLs.

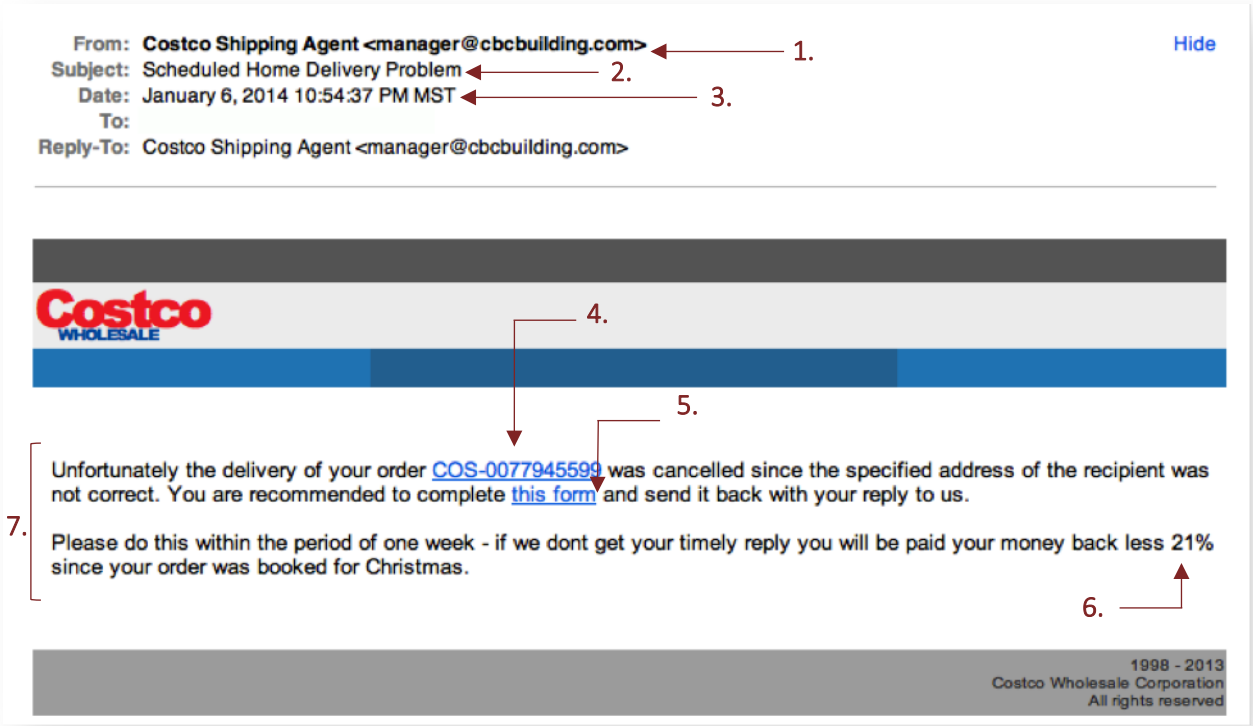
It should be noted that this is not a complete list of phishing tactics. In fact, the methods of cyber-criminals continue to evolve, opening the door for larger and more effective attacks. Phishing isn't going away anytime soon and, because it is so difficult to counteract, it's critical that you know a number of methods for spotting and preventing common scams.

Spotting an Attack

When it comes to identifying phishing scams, it's better to be overly cautious. While recognising fraudulent emails and websites can be difficult, depending on the type of attack and the creativity of the phisher, the following are some questions to ask yourself whenever you receive a suspicious email:

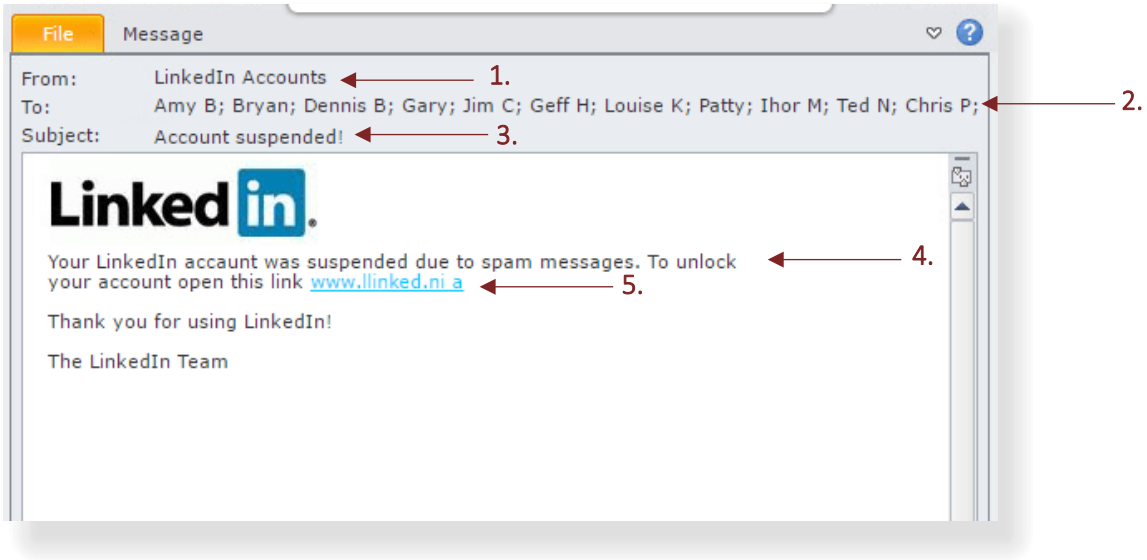
- What time was the message sent? You can tell a lot about the authenticity of an email based on when it was sent. For instance, an email sent at 3 a.m. would raise more flags than one sent during normal business hours.
- Do I know the sender? It's a good idea to look closely at who sent a particular email. Ensure that the 'From:' field matches the sender's name. If an individual claims to know you and you don't recognise them, chances are the email is spam.
- Do the URLs match up? Advanced phishers create fake domains to mimic larger, more established companies. For instance, a cyber-criminal may send you an email hoping to redirect you to a phishing website. This website will have a convincing URL that's only slightly different from the original website, like www.bestbuy1.co.uk or www.1target.co.uk.
- Does the content match the subject? Read the email carefully. If the subject line is vague or does not seem to relate to the body copy of the email, it could be a fake. Subject lines may appear aggressive or urgent. Many times, these subject lines are written with strange capitalisation and punctuation. Globally, the following were the subject lines of the most clicked phishing emails in recent years:
    a. Security Alert
    b. Revised Holiday & Sick Time Policy
    c. UPS Label Delivery 1ZBE312TNY00015011
    d. BREAKING: United Airlines Passenger Dies from Brain Haemorrhage – VIDEO
    e. A Delivery Attempt was made
    f. All Employees: Update your Healthcare Info
    g. Change of Password Required Immediately
    h. Password Check Required Immediately
    i. Unusual sign-in activity
    j. Urgent Action Required
- How is the grammar and spelling? Large companies dedicate time and money to their communications. Because of this, spelling and grammar mistakes in legitimate emails from global brands are rare. Be sure to read emails carefully and be wary if there are consistent, glaring errors.

Example Emails



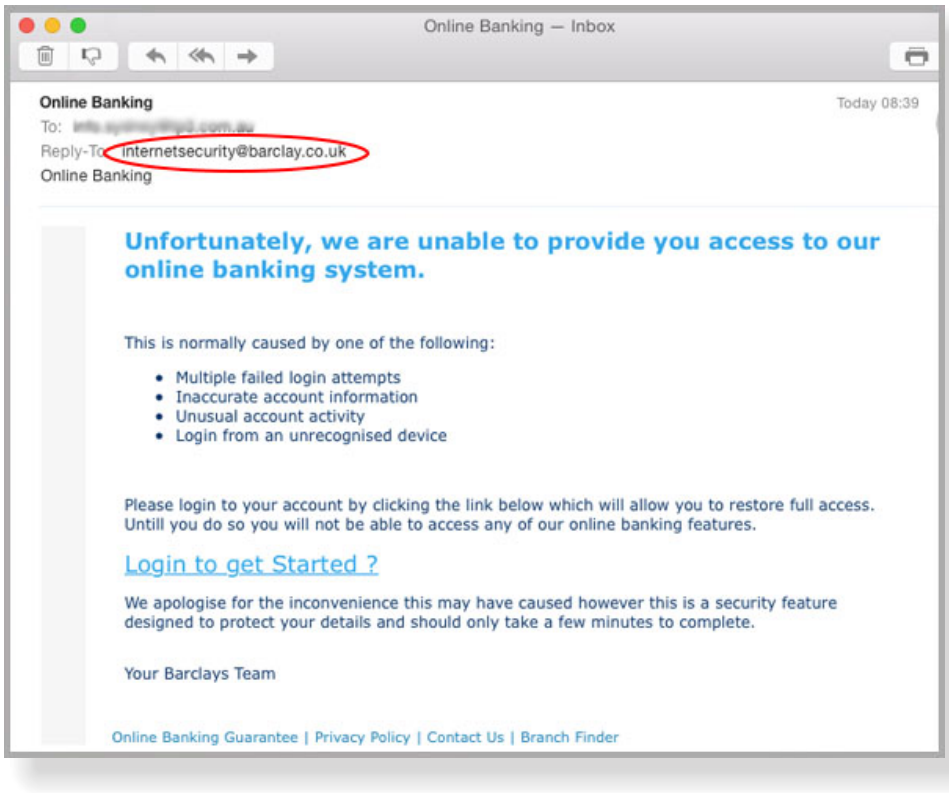
Issues with This Email

1. The 'From:' field (manager@cbcbuilding.com) does not match the sender, Costco.
2. The subject line is vague and uses scare tactics. Be especially suspicious of this kind of email if you don't know what the message is referring to (eg, you don't remember making a specific order).
3. The sent time is nearly 11 p.m. While automated messages may fall outside business hours, companies tend to distribute emails during time periods you are most likely to open and read their messages.
4. Whenever a message references a specific order number or code, it's important to cross-reference it. Navigating to a company's legitimate website, logging in and checking your order history is a good way to confirm that order-related emails are real.
5. Companies will rarely redirect you to separate landing pages. A good way to check if links are legitimate is to hover over them. Doing so will show you where the link directs you. If the URL doesn't appear to relate to the email or the sender, do not click it. If you recognise the sender, reach out to them offline and ask if they meant to email you. Be sure not to reply to the potential spam email and, instead, use a different contact method.
6. Watch out for emails that use specific figures as scare tactics. Ask yourself, would a legitimate company give you a quick turnaround time and reference specific losses through an email?
7. Read the body copy of the email carefully, looking for odd verbiage and spelling mistakes. In this example, the sentence 'You are recommended to complete this form and send it back with your reply to us' stands out. For some phishers, English is not their first language, making errors like these common.



Issues with This Email

1. The 'From:' field is general and doesn't display a legitimate email address.
2. The 'To:' field contains multiple email addresses. If a single account was compromised, legitimate companies wouldn't notify multiple people at once.
3. The subject line is vague and uses suspicious formatting and punctuation.
4. The body copy is broad and doesn't reference specific accounts. When receiving messages of this kind, contact customer service using numbers listed on official websites.
5. The link www.llinked.ni.a contains a suspicious domain (.ni.a) and is not obviously associated with the official company, LinkedIn.



Issues with This Email

1. The design of this email is unprofessional and features no branded elements. Organisations are serious about their digital marketing practices and the customer experience. Because of this, correspondence from real companies is often sent using professionally designed and edited templates.
2. The body copy includes multiple grammar issues, odd phrasing and a number of scare tactics. Additionally, the text of the email does not include any account specifics or personal information. This indicates the message could easily be sent to many individuals at once.
3. Just because a message says a link is secure, doesn't mean it is. Again, companies won't usually redirect you to outside websites, instead instructing you to contact them via phone or other official means.

Avoid Becoming a Victim

As a basic rule of thumb, if something seems off about an email, do not click any links within the body copy or download attachments.

The following are some other tips to avoid becoming the victim of a phishing scheme:

- Be overly cautious of suspicious emails, deleting them immediately. Be particularly wary of emails that:
    - Come from unrecognised senders
    - Ask you to confirm personal or financial information
    - Aren't personalised
    - Are vague
    - Include threating, frightening and persuasive language
- Never enter personal information or click links in a pop-up screen.
- Avoid emailing personal or financial information, even if you think you know the sender.
- Hover over and triple-check the address of any links before you click them.
- Avoid replying to the sender if you suspect an email is malicious. If you recognise the individual or company sending the suspicious email, follow up with them offline to ensure they meant to contact you.
- Report the attack to your employer and the proper authorities. Regardless of the region you live in, all suspected scams should be reported to Action Fraud.
- Verify a website's security. Legitimate websites will have a URL that begins with https, and you should see a closed lock icon somewhere near the address bar.
- Review your online accounts regularly and use different passwords for each one. Most importantly, review your bank and credit card statements to ensure that all transactions are authorised.
- Keep your browser up to date and use firewalls.
- Run antivirus and anti-malware software on a regular basis. Reputable venders include McAfee, Symantec, Malwarebytes and Avast.

Additional Considerations for Employers

While the above prevention tips are important, there are additional concerns for employers. A company could have the most top-of-the-line cyber-security measures and still fall victim to phishers. Just one employee opening a malicious email can compromise an entire network. To protect themselves, businesses need to do the following:

- Implement a data protection programme. Train employees on common phishing scams and other cyber-security concerns. Provide real-world examples during training to help them better understand what to look for.
- Segment networks if possible, keeping sensitive information separate. This can help prevent the loss of an entire network should one employee fall victim to a phishing attack.
- Filter emails and websites.
- Take advantage of protective practices such as pseudonymisation of employees' and customers' personal information or data encryption. This way, even if a hacker gets their hands on sensitive material, they will have a harder time translating it or making use of it.
- Have employees use unique usernames and passwords. In instances where employees share credentials, hackers can cause major damage to your business simply by compromising one employee.

Get Informed, Stay Protected

Cyber-attacks, including phishing schemes, aren't going away. In fact, they're becoming more sophisticated. It's no longer enough to simply install antivirus and anti-malware software. To truly protect yourself, it's crucial to stay informed on the most recent cyber-attacks and up-to-date protection strategies.

In addition to providing risk management tips for both employers and individuals, Sutcliffe & Co. Insurance Brokers can help keep you informed on the biggest happenings in cyber-security and provide robust insurance solutions. Contact us today to learn more ways to stay cyber-safe.