Phishing Attacks: What are they and how to avoid them

What is a Phishing Attack?
A Standard Phishing Example
Popular Phishing Attacks in 2022
The Habits of Attackers
The Damage They Do
Protection and Prevention

What is a Phishing Attack?

"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself." – Sun Tzu

Phishing is a type of social engineering. Malicious attackers send emails or messages intended to trick users into giving away information like passwords, personal information, or account numbers in order to gain access to systems. Once they have this information it can lead to the installation of malware, revealing of sensitive information, or a ransomware attack.

For a private individual this often means that they give away information that allows the attacker to make unauthorized purchases, steal money from various sources, or outright identity theft. In the corporate world however, they are more often used to gain access as part of a more ambitious attack. Compromising employees in an organization allow these attackers to bypass security measures, install and distribute malware inside a closed system, or even gain access to secure data.

The financial losses associated with such an attack can be severe. Not only directly but also through reputation and consumer trust, but also potentially through declining market share. If the scope is large enough, the security incident can be difficult to recover from.

First and foremost, it is important for an organization to keep up with and understand the variety of types of phishing attacks that are out there. Understand what methods are used, and keeping employees up to date on these methods, is an important method for protecting your systems.

There are other methods for avoiding phishing scams as well.

Your digital footprint extends well beyond your internal corporate network. Cloud-based computing and business partnerships touch your network and provide access to your systems as well, so considering their security is equally important. Be aware of what your partners, contractors, and suppliers are giving away about your organization.

Relying solely on employee education isn't enough to secure your systems. It is an impossible request and is detrimental to productivity. Systems that can be set up to keep a watchful eye on email, such as email filtering services are a good intermediate step.

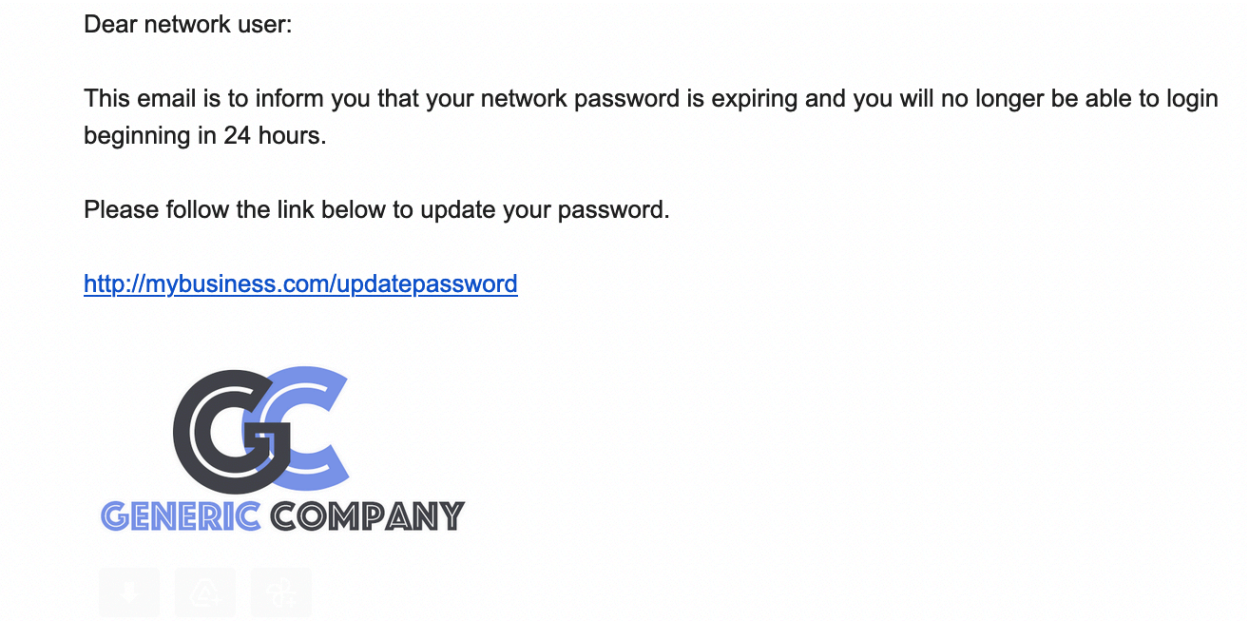
Reporting fraudulent email scams to your businesses local government oversight organization is also useful. Not only can this protect you in the future but other businesses as well. Stopping attackers who are actively working on knocking down digital doors is a benefit to all.

Recognizing a phishing attack attempt is the first step. The attackers are always coming up with new tactics, so staying abreast of their methods is imperative to protecting your company's data security.

A Standard Phishing Example

"When one treats people with benevolence, justice, and righteousness, and reposes confidence in them, the army will be united in mind, and all will be happy to serve their leaders." – Sun Tzu

In this example it appears as though your own business is requiring a password change. Employees may not even really think about what they are about to do. The link will appear fairly normal but be disguised and take the user to an entirely different website that will appear to walk them through a password reset.



Although it often may seem reasonable, to some, that this type of phishing attempt is obvious, people fall for them frequently. Remember, phishing relies on social engineering and the expectations and habits of everyday people. Employees may not even think about clicking on a link in an email or message like this one.

It should be noted, punishing employees for making the mistake of clicking, getting caught causing an issue, is not recommended. This will further discourage employees from reporting in the future and potentially cause them to scrutinize every single email and message more than needed, creating a loss in productivity and excess paranoia. Both things cause more harm than good.

Popular Phishing Attacks in 2022

"Do not swallow bait offered by the enemy." – Sun Tzu

The essential formula behind phishing attacks is using psychological tricks, social engineering, natural human behaviors, and things people do nearly automatically without thinking. The attackers use these methods because it makes them hard to detect by humans and software which in turn allows them to steal sensitive information and/or credentials, often using fake links or malicious attachments.

Lack of up-to-date awareness is a big problem, because attackers rely on this missing knowledge and habitual behavior to accomplish their goals. This makes users, and therefore your business, more susceptible to these threats.

Standard phishing emails and messages generally represent themselves as a reputable source or organization, often your own, a partner organization, or a familiar brand. The most effective of these uses current issues and events that most people are aware of to trick people.

Using the Pandemic

Two years of battling the pandemic has created a new opening for phishing attackers. Because it is of concern in every home and in every field of work, it is much easier for cybercriminals to use it as a clever method to gain access to systems. According to Check Point researchers "…cyber-criminals are exploiting interest in the global epidemic to spread malicious activity…" and they are finding great success doing so. The fears and misconceptions people have about COVID-19 have opened a whole new entry point.

These attackers are constantly updating their methods and clever messaging. Use this as a reference guide and starting point to help identify the types of pandemic-related phishing you and your employees may come across.

- Emails that spoof or impersonate the World Health Organization (WHO)

  These emails often will include subject lines asking for donations or warnings about taking precautions. An attachment or link can be clicked on including the phrases like "Virus Protections" or "Donate to the Pandemic Response Plan" will be included. Once it is clicked on it will infect the system with malware.

  The World Health Organization has said it will never ask for donations to emergency plans via

email, websites other than their own (WHO), calls, or text messages.

- Emails that advertise or promote fake COVID-19 cures and treatments

  A cure or miracle treatment would be wonderful, wouldn't it? You will hear about it on the news before you hear about it in a random email. Conspiracy theories are common, especially in times of great concern and panic. Too good to be true is one of the things these theories thrive on. Remember than when one shows up in your inbox before it shows up on a legitimate news source.

- Emails with fake medical test results

  Frequently targeting healthcare industry companies, these emails contain a link or an attachment labelled "test results." When it is clicked on malware will be installed on your system.

- Emails targeting work from home employees

  Taking advantage of the many more people working from home since the beginning of the pandemic, cybercriminals have found that impersonating company higher-ups or even the HR Department can be useful. Tricking these remote workers into signing into a spoofed system on a website and thereby giving away their login credentials.

- Emails impersonating your local health department or ministry

  It could be your state health department, a county health department, or another local health organization with official standing. Many of them contain an informational document as an attachment, or possibly a link to click on, that once opened will install malware that can allow the attackers access.

Customs and Delivery Services

Delivery services, customs services, and even postage sales phishing emails are popular and have been making the rounds. Attackers and scammers send emails and messages designed to look like package tracking or ask for payment of a fee via a malicious link.

Often these messages will be designed to look like a legitimate package or customs service that may be familiar to you or your employees. Claiming to have failed a delivery attempt or announcing customs fees are common tactics in these emails. Attackers may also send a message that offers tracking of a package that you or your employees do not remember ordering.

Invoicing and Finance-Related Emails

Targeting financial employees has become more common in 2022 as well. Using their sense of responsibility to stay on top of investigating and checking payment issues, these emails can look very normal to this specific set of employees. Fake links and attachments, sometimes PDFs, to steal credentials or install malware, they are designed to look very official and blend in with all the other emails financial employees see every day.

Urgency is an important and useful tactic that scammers and cybercriminals use to socially engineer their way into systems. These targeted finance phishing emails will often use phrases such as “overdue notice,” or “update payment details.”

Using Taxes

Taxes for companies are dealt with, one way or another, year-round. Phishing messages using official tax entities or tax organizations become more common during tax season but can happen year-round. Look for these and remember that no one should be asking for information like Tax ID, Social Security Numbers, banking details, or other confidential financial or tax-related information via message or email.

Always double-check and investigate emails claiming to be from a taxation organization. Even if you are waiting for a refund, subsidy, or other information from your tax office, check with them on the status.

Phishing emails using taxes in an attempt steal information or install malicious code on your systems often use subject lines like “Tax Refund Due,” “Tax Account Restricted” or “Update Tax Information.”

Impersonating a Recognizable Brand

An oldie but a goodie, impersonating a well-known brand is one of the most common, and one of the most successful, methods attackers use when phishing via email. It is just as popular as ever.

The most popular brand to impersonate is Microsoft, which makes sense, especially in the business world. Microsoft is ubiquitous in offices and on work computers. Almost everyone uses a Microsoft product at work one way or another.

Phishing attackers also impersonate other brands. Facebook is a very close second behind Microsoft. It is still the most used social media platform in the world. Other popular brands that are frequently impersonated are Crédit Agricole, WhatsApp, Orange, Paypal, and Google. Other very common brands that get impersonated are Norton, McAffee, Apple, and Amazon.

Malicious actors use these recognizable and trusted brands to trick users into giving out enough of the right confidential information or to click on links or attachments that are in the email. Inconsistences or unexpected messages should be double-checked.

Checking with the brand immediately via their contact details on their websites is a good idea. Often these emails will be asking for a password reset when one wasn’t requested by you or your employee or asking for an update of payment information on the existing account.

The Habits of Attackers

"It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for the purposes of spying, and thereby they achieve great results." – Sun Tzu

Phishers do have preferences and habits. They tend to attack certain types of industries and attack on certain days of the week or certain times of day. They prefer types of brands to impersonate (see above) and they rely on the same types of language in their attempts to trick users into clicking on links and attachments. Staying informed and understanding these tactics and habits gives you a leg up on preventing the likelihood that they will be successful with your systems.

Targeted Industries

The financial sector is the most targeted industry. According the research done by Statista nearly a quarter of all phishing attacks worldwide are directed at financial institutions. The financial sector is closely followed by web-based software (SaaS) and webmail services. Other industries popular with phishing attackers are E-commerce/retail, cryptocurrency, and logistics and shipping.

When Do Phishing Attacks Happen?

It is impressive how cybercriminals have figured out what days of the week, and even what times of day, people are most likely to fall for their trickery. Weekdays are most common, with Monday through Wednesday being the most popular, and activity dropping off Thursdays and Fridays. A significant drop-off in activity occurs on Saturdays and Sundays. Phishing emails tend to arrive four to five hours after start of business and peak around lunchtime, right when everyone is just getting into the swing of things and starting to do things just a little out of habit. Perfect timing.

Phishing Language Tricks

Learning how the phisher communicates is important. Educating your employees, and yourself, about the way they communicate can help protect your business. Phishing uses the content of an email or message to encourage the reader to perform certain actions; they need us to do the real work for them.

It is a psychological trick. Communicating in the right way can use human emotion and behavior to cause action. It is not lost on these internet criminals that language matters and they can use language to cause the recipients of their messages to act.

There are many groups and research organizations that keep track of various hacking and phishing campaigns. One group, the Anti-Phishing Working Group (APWG) keeps an eye on the behaviors and activity of phishing groups worldwide. One of the many things they track is the subject lines and language content of the emails and messages phishing attackers send.

For example, during the height of the pandemic and since the APWG found that a common phrase used in phishing emails is “expires in 2 days.” This plays on a sense of urgency and encourages immediate attention to the email.

Over the years researchers have determined the most common words used in phishing emails. The top words include words that also show up in legitimate emails all the time. The top five are “label,” “invoice,” “post,” “document,” and “postal.” Considering this use of commonly used words, it is important to remember that words and language *in addition to context* matter.

All About the Context

Because a combination of context and language matters, let’s take a look at the themes and context of phishing emails.

- They portray a sense of urgency

  For example, pressuring the recipient of the email to change a password or verify something immediately.

  “Your password has expired. Please update your password now to maintain access to Office 365”
  “A vulnerability has been detected in your Facetime mobile application. Please verify your account now.”

- Fear of missing out (FOMO)

  FOMO can be highly effective in phishing emails. For example:

  “Don’t miss out on this once in a lifetime offer… “

- Authority (mixed with urgency)

  Spoofing the name of a CEO or other high-level authority figure in a company is not uncommon.

  “Beth, I need you to process this transaction ASAP. It needs to be done today or we will lose this new customer.”

- Emotion

  A tactic often used in sexploitation campaigns. For example, “you’ve been recorded while using a porn website…”

THE DAMAGE THEY DO

"*If you know the enemy and know yourself, you need not fear the result of a hundred battles*." – Sun Tzu

Phishing is on the rise. According to Ironscales, a company that specializes in email security, 81% of organizations worldwide have experienced an increase in phishing attacks since 2020. In fact, various reports and research have found that recently the attacks have been focused more on stealing credentials in order to breach a system rather than installing malware. Google Safe Browsing has reported that phishing sites are becoming vastly more common than they were previously.

All these attacks and attack attempts out there can be incredibly costly for a business. The financial consequences can be quite dire.

IBM reported in 2021 that the cost of a data breach is, on average, 4.24 million dollars. This figure is higher than it was for the previous year, which is an indication that these breaches are becoming more financially dangerous over time. However, it is interesting to note that IBMs study also showed that there is an increasing gap in cost of a breach between organizations that have more advanced security processes in place and those with fewer.

Phishing scams are some of the costliest attacks, according to information reported by the FBI's Internet Crime Complaint Center. What this all comes down to is that social engineering attacks are costly and getting more so every year.

Costs and financial damage done by a successful phishing attack can be broken down into categories.

- Direct monetary losses
- User downtime
- Loss of intellectual property
- Remediation time and associated costs
- Compliance fines
- Loss of revenue and customers
- Legal fees
- Damage to reputation

It is worth considering that the costs of a successful attack are not simply financial.

A successful phishing attack can lead to a multitude of issues for your business including:

- Lost data
- Compromised accounts and credentials
- Damaged reputation
- Malware infections
- Ransomware

Lost data is a key cost when a breach has occurred. The types of data that are most often compromised during a phishing attack are:

- Credentials: Usernames and passwords to various systems
- Personal data: Addresses and phone numbers stored on your systems
- Internal data: Sales figures, financial data, customer data
- Banking data: Credit card information, bank account information
- Medical data: Insurance claim data

Protection and Prevention

"In battle, there are not more than two methods of attack--the direct and the indirect; yet these two in combination give rise to an endless series of maneuvers." – Sun Tzu

When it comes to ensuring your business is as protected as possible, a multi-layered approach is best. There are technical solutions available that can keep an eye on things for you via your IT department. Human-centered defense is also very important. Phishing is especially social, using emotion, clever language, and relying on turning the recipient of a message into an unknowing accomplice. The better the humans at your business are at recognizing these tactics the better.

Security and password management

Using systems that manage password security as well as access protection in addition to security systems that require Two Factor Authentication (2FA) for logins are always a good idea. In the event of a security breach, something like 2FA can offer an extra layer of protection that prevents an outside attacker from knocking the door down. While password management, while not a perfect solution on its own, can ensure that employees are not using the same password repeatedly, which is a surefire way to mistakenly allow a good social engineering attacker into multiple systems.

Security Awareness Training

Because phishing emails all have common tactics, common language, and common themes, they have a weakness. By educating your employees about these commonalities in phishing messages, you can help them identify a malicious attack before they click on a dangerous link or open an infected file. Your employees can be a critical part of your defense against attacks.

A security awareness training program is a good way to transform your employees into one of your layers of defense. Security awareness programs or phishing awareness training programs provide and deliver engaging simulations and training so your employees company-wide can learn how to recognize, without endangering anything, how these attackers really work.

A 2022 report from Cofense, an organization dedicated to stopping phishing attacks, found that employees who completed a security awareness training program were much more likely to report and

detect a phishing attempt. From their own simulated campaigns, Cofense reported that 82% of employees that had completed training reported a simulated phishing attempt within an hour, more than half reported the simulated attempt with 5 minutes, and nearly 20% reported the attempts within 30 seconds.

Using your trained workforce as a defense against phishing is a clear benefit. A very important part of the multi-layered defense against phishing. People alone cannot do all the defending in this case. You need serious help from technology. The attackers are using technology. You should be too.

Secure Email Gateway

A Secure Email Gateway (SEG) monitors your incoming and outgoing email. It simply scans them for malicious content. If the SEG detects any spam, malware threat, or phishing attempt that it recognizes, it quarantines or blocks the email from getting through.

This layer of protection is important as it can catch a good number of mass phishing attacks. As long as it is kept up to date, so it has the latest information for generic attempts at phishing, spreading malware, and spamming, a SEG does a pretty good job.

A vulnerability to SEGs is that they will not catch spoofed email messages. Any message that is impersonating a known sender will make it through, for example. In order to defend your data and systems against these more individual types of attacks, you need another layer of technological protection.

Cloud Email Security

This level of protection against phishing sits within your email network itself and monitors all inbound, outbound, and internal messaging for malicious content. Using AI and machine learning, cloud email security analyzes each user's communication patterns and behaviors and then scans for anything out of the ordinary.

Well Rounded Security

Ensuring your business or organization has as much protection set up as possible is key to preventing the worst of scenarios. A robust multi-layered defense means finding the right training program for your workforce, staying informed yourself, and doing everything you can with technology to filter and monitor email communication as well as keep those passwords and credential safe.