White Paper

Social Engineering:
What you need to know to stay resilient

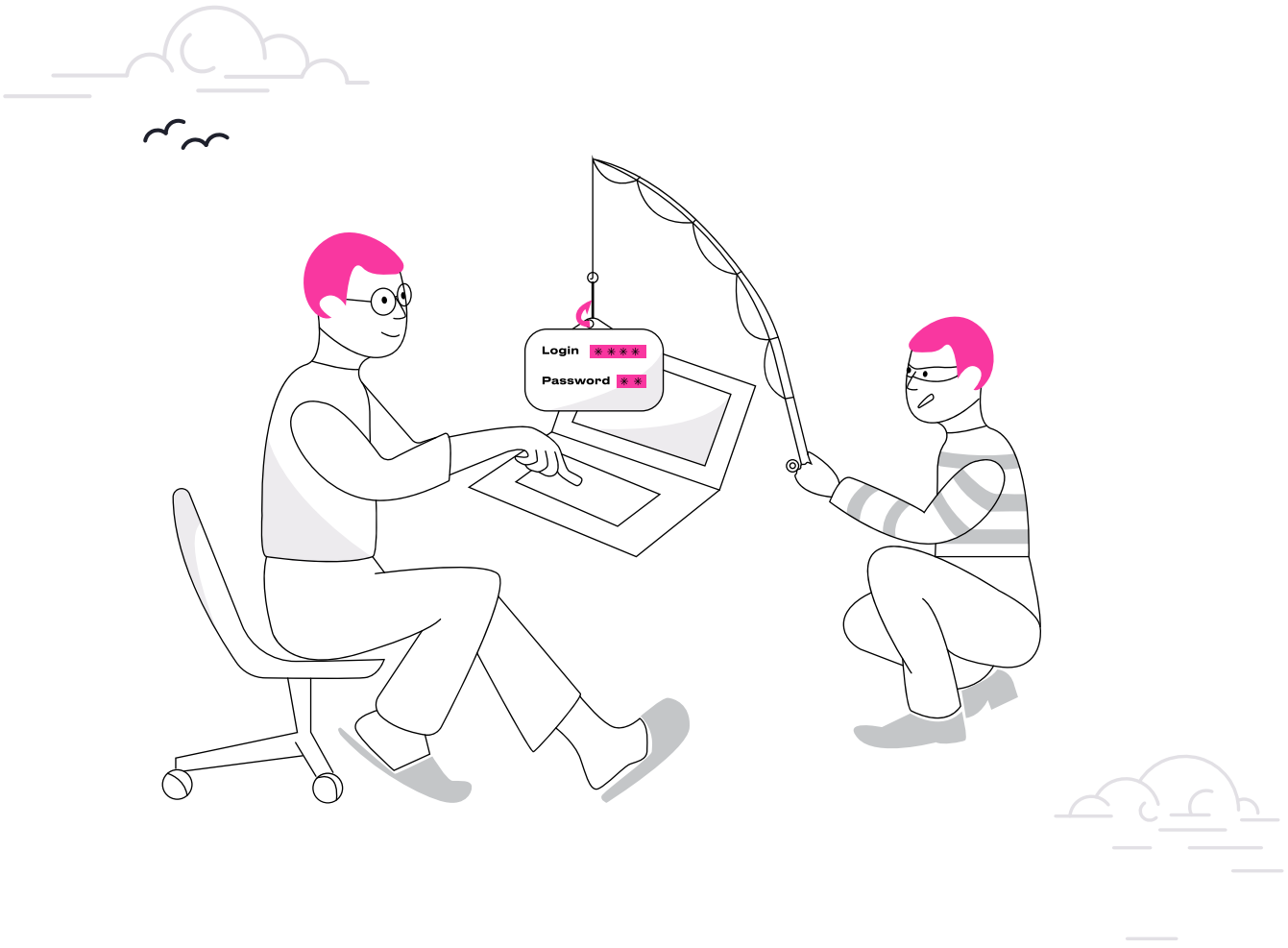
By Adam Bar Zeev

Contents

Are you familiar with the term, “social engineering”? If not, here’s another question for you: Have you ever received an email with a subject line saying, “You won!” or an email claiming, “Your password is about to expire. Click here to update it?” Both are classic examples of social engineering.

Social engineering are tactics designed to trick end users into doing something potentially harmful, like giving away their credentials to company logins and SaaS applications.

In this white paper, you’ll learn what social engineering is, the common tactics used in this type of attack, how social engineering is evolving, and what you can do to stay resilient against these attacks.



Social engineering 101

Social engineering is the art of manipulating, influencing, or deceiving by exploiting human vulnerabilities or moral principles. Malicious actors use social engineering to access a system or steal vital personal or company information. This could be physical access to a company's building or computers, digital access to a system or server, or anything in between.

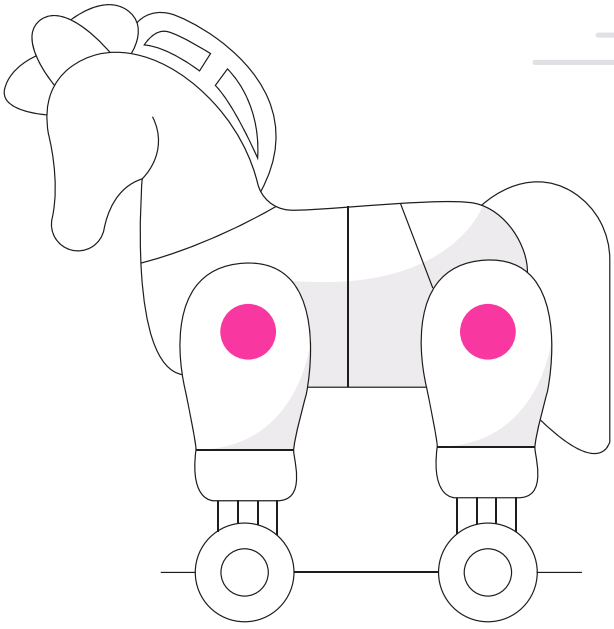
Recent research shows that cyber criminals use social engineering in 98% of attacks.

Why social engineering?

Cyber criminals find it's easier to manipulate a person rather than using technical "hacking" actions, like exploiting software vulnerabilities. Most of the time, the motivation is money. By getting their hands on sensitive information, they can make a big profit by selling stolen information or withdrawing money from accounts.

While it's a simple tactic, implementing social engineering isn't as easy as it sounds. Effective social engineering campaigns require extensive planning. What used to be a quick "get rich" tactic for bad actors is now a primary technique used by threat groups to cause considerable damage to businesses and industries.

That's why understanding what social engineering is, its history, and how it is evolving is key to protecting your organization and its end users. (And you should probably share this with friends and family too.)



A history lesson

The lesson of the Trojan Horse

Let's briefly go back in time to one of the oldest and most famous social engineering attacks. The year is 1184, and it's the tenth year of the war between the Greeks and Troy. A towering wall protects the city of Troy, and the citizens never let foreigners in.

For ten long years, the Greek warriors attempt to breach the Trojan wall with no success. In order to break the stalemate of the long war and put an end to the bloodshed and pain, Odysseus produces a cunning plan.

The Greeks build a spectacular and huge wooden horse as a "gift." Then they make it appear as though they've sailed away, leaving the horse as a peace offering. At first, Troy is hesitant. But after debating and the obvious fact that the Greeks had left, they decide to accept the gift.

What the people of Troy don't know is that lethal soldiers of the Greek army are hiding inside the wooden horse. The people of Troy drink and celebrate their victory all night long. Then, late at night, when all the people of Troy are deep in sleep, the Greek soldiers spring out of the wooden horse, open the city gates, and let in an army of Greek warriors.

All it took was the city of Troy letting their guard down. Once the Greeks had a foothold and opened the city gates, there was no turning back. That was the end of Troy.

The legend of the Trojan Horse is a classic example of a dedicated, well-planned attack. It includes strategic thinking, deception, and patience – waiting for the perfect moment to strike. That's social engineering.

Animal Program – 1975

In 1975, the first Trojan malware spread throughout the world. Programmer John Walker created the program "ANIMAL," a game designed to guess the animal that the player was thinking about by asking 20 questions.

The game was considered the first Trojan because it had a hidden functionality. It examined all the computer directories the user had access to and copied itself to any directory that it wasn't already in.

The program didn't execute any malicious content, nor was it harmful to the computer. But it did have the dangerous ability to spread to other directories. Modern malware campaigns are derived from this idea.

Kevin Mitnick

Over the years, social engineering evolved alongside technological developments. In the 1990s, Kevin Mitnick, one of the most wanted hackers in the US at the time, attempted to leave the country before he was arrested.

To hide himself, Mitnick needed to find a way to communicate privately without being located. Realizing he might be located through data exchanges from cell phone towers, he got an idea to change the identifying data on his phone. To pull it off, he needed to get his hand on the source code of the Motorola MicroTAC Ultralite (which was a popular cell phone in the 1990s).

Mitnick started executing his plan by calling a directory assistance to get Motorola phone number. Once he called the Motorola call center, he asked for the MicroTAC Ultralite project manager. After being transferred eight times, he finally reached the Motorola Vice President for all Motorola mobility. During the call transfers, Mitnick gathered information and learned that Motorola had a Research Center in Arlington Heights. Knowing this, he impersonated an employee that worked in the Research Center. He managed to get ahold of a VP, who gave Mitnick the extension number for MicroTAC Ultralite's project manager.

He called the extension and found out the project manager was on vacation according to her voicemail. The voicemail informed callers that "for any help whatsoever, call Alicia on the following extension..."

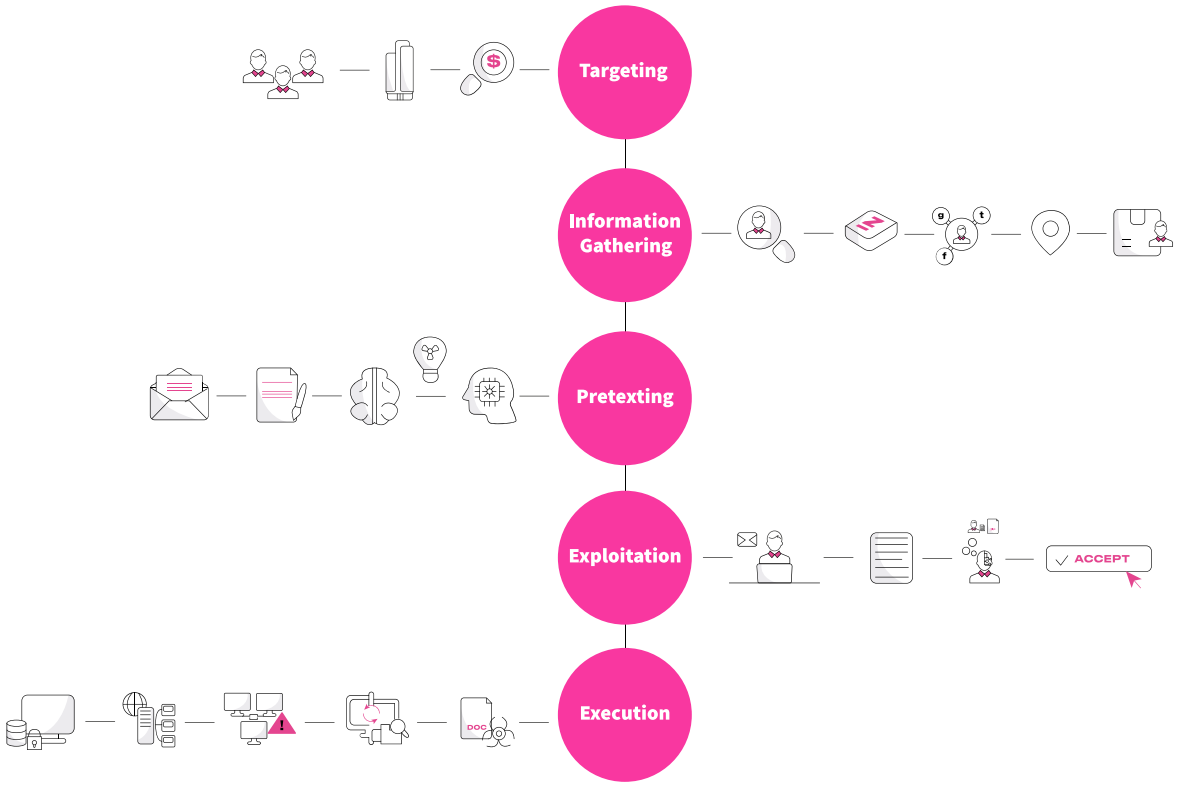
Poor Alicia.

Using the art of social engineering, Mitnick manipulated Alicia into trusting him. He guided her through taking source code, zipping it, and transferring it via FTP to an anonymous FTP server.
Within a few simple phone calls, he succeeded in using social engineering to get Motorola staff members to help him complete his plan.

Mitnick had his hands on the Motorola MicroTAC Ultralite source code. In case you're wondering – yes, he got busted and went to jail.

The stages of a social engineering attack

The important thing to learn from social engineering's history is that there are always crooked people trying to take advantage of others for personal gain. To help you protect yourself and your company, we'll review the stages of a modern social engineering attack.



Step 1: Targeting

Threat actors start by identifying a target. Usually, they target companies. And the most efficient way to breach a company? Through its employees.

The threat actor may choose a company they're already familiar with. For example, an attacker might learn that their friend's brother works at a place that doesn't have a system or supervisor that checks for ID/security cards or fingerprints. This kind of information is gathered and used to build a plan based on vulnerabilities.

Another good example of having an "in" is when a threat actor hears the conversation of two random people in public talking about how their company does not use security products or that cybersecurity awareness is low. Targeting can take place in multiple ways, from physically scouting workplaces for any sensitive information to using leaked data found online.

Step 2: Information gathering

Once the target has been selected, the next step is reconnaissance, or collecting as much information as possible. Open-source intelligence (OSINT) is the practice of gathering information through overt and publicly available sources across the internet with the use of OSINT tools and skills.
When you're not sure about something, you search for it online. We all know the saying: "Just Google it."

Threat actors do the same, though in a much more sophisticated manner. Valuable information can be found in employees' social media accounts, forums that they're registered to, and more. The information they find is used in the next step of the chain.

Step 3: Pretexting

After completing their homework, it's time for these bad actors to strategize. Pretexting is a form of manipulation, which involves fabricating or inventing a scenario to trick the target into divulging information or performing an action. The main goal in the pretexting stage is to build trust between the threat actor and the victim without causing suspicion. Threat actors write sophisticated messages, impersonate coworkers, and fabricate complete situations from A to Z. Once the trust has been built, threat actors carefully take advantage of this new relationship.

Step 4: Exploitation

After a relationship has been built, threat actors will manipulate their target and attempt to steal sensitive information like credentials, finance/banking details, and personal data. In some cases, the threat actors will trick the victim into visiting unknown URLs, downloading unknown source applications, opening emails that have a malicious Microsoft Office document attached, etc. These actions give the threat actor initial access to a victim's computer or company environment.

Step 5: Execution

This stage is where the threat actors achieve their end goal; it could be financial, political, or personal. In this step, threat actors use their newly found access to infect the target environment with malicious content, which will eventually lead to a compromised network. In the process, they steal banking information, harvest credentials, and deploy ransomware. The threat actors then make a profit from the stolen information by withdrawing money from accounts or selling sensitive information on Darknet forums.

The different methods of social engineering

In the past two decades, technological advancements have opened the floodgates for new social engineering techniques. These advancements include things like email, SMS (short message service or text message), public Wi-Fi, Internet protocols, USB devices, smartphones, smartcards, cloud infrastructures, and more.

In the modern workplace, where technology and computers are everywhere, bad actors have all kinds of means to find their “in.” It’s vital to recognize the different types of social engineering attacks and techniques to protect yourself.

Below are some of the most common techniques, differentiating between two main types of attacks: physical social engineering and computer-based phishing.

Physical social engineering

Dumpster diving

Dumpster diving refers to searching for information by snooping around in the trash of a person or business to gather sensitive physical, sensitive information like ID numbers, documentation with personal identifiable information, financial info, business numbers, etc.

Mail theft

Similar to dumpster diving, mail theft involves targeting a physical mailbox. The threat actors look for pertinent/sensitive information, finance/bills, and payment documents.

Eavesdropping

Gathering info by listening to conversations without approval.

Shoulder surfing

Looking over a person's shoulder in order to view any valuable/sensitive information like passwords, credit card numbers, pin codes, etc.

Impersonation

Acting as a legitimate employer/user or a person with authority to gain access to information or a system. No, your CEO doesn't really need you to buy gift cards for them.

Piggybacking

Attempting to enter a physical environment, such as an authorized building/department/room that requires authentication (smart badge/fingerprint authentication). In most cases, the threat actor will impersonate an employee who has forgotten their badge or make up another story.

Tailgating

Tailgating has the same goal as piggybacking but doesn't involve direct contact. Once an employee enters their business, the threat actor will take advantage of that opportunity (like slipping through a closing door) to sneak into the space without the employee noticing.

Phishing

Phishing is the most common social engineering type of attack. It involves “baiting” users into doing something harmful. Phishing attacks are most commonly emails with malicious files disguised as something legitimate or beneficial. Over the years, the definition of phishing has changed, and new sub-categories have developed based on the different phishing approaches spotted in the wild.

Spear phishing

Spear phishing is a targeted phishing attack. Targets can be people, groups, workplace departments, organizations, etc. Spear phishing is more strategic than general phishing, which typically involves spamming email inboxes across the organization.

Smishing

Smishing stands for short message service (SMS) and phishing. In smishing, a text message is sent with a URL directing to a website. The website may seem legitimate and part of an official organization, but in most cases, it’s a phishing website that will steal your credentials, financial information, credit card numbers, etc.

Vishing

Vishing stands for voice phishing attacks via a voice communication channel, usually a phone. It involves manipulating victims to reveal personal and sensitive information, like debit card numbers. Vishing is prevalent in the world of mobile phones and VoIP (Voice over Internet Protocol) — including popular conferencing tools such as Zoom, Microsoft Teams, Skype, Discord, etc.

Watering Hole

Water holing is a social engineering technique where attackers infect a website that their targets frequently visit. By infecting the website with malicious files, attackers gain an access point to their victims’ information.

Clickbait

Baiting, or clickbaits, are popular social engineering attacks that exploit curiosity, tempting the victim to click on a link thanks to clever text copy. Clickbaits come in the form of advertisements on websites, posts on social media platforms, emails, and more. They use promising headlines like, “You won’t BELIEVE what . . .” or “Get your free gift!” When people click these links, they are usually clicking on malicious redirecting URLs or masqueraded JavaScript objects.

The evolution of phishing

Phishing is among threat actors' favorite methods for stealing credentials and spreading ransomware. In fact, according to the FBI IC3 2021 report, phishing is in the top five crime types. When a significant portion of the workforce quickly shifted to remote work in 2020, there was a sharp increase in phishing attacks.

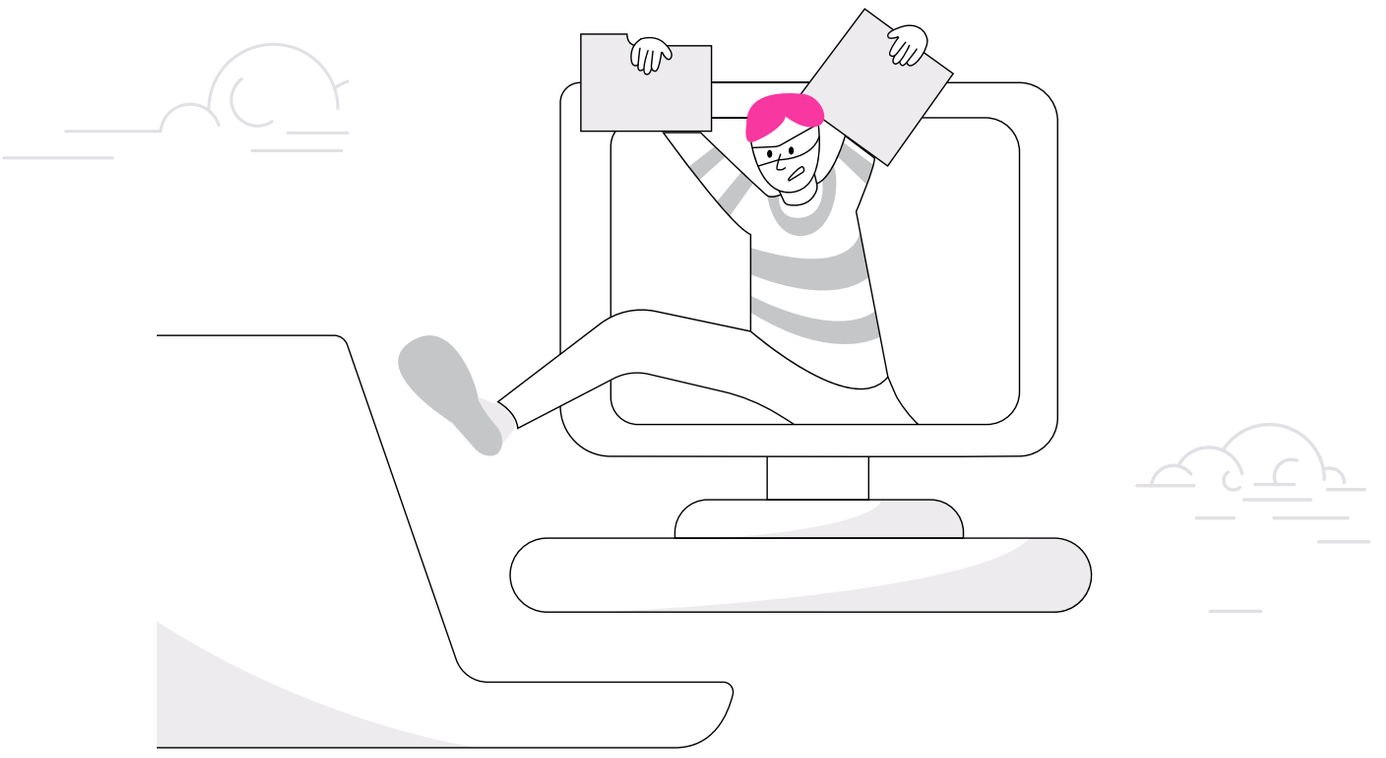
We've all seen them. Phishing emails use trending topics, targeted subject matter, common subject lines, and text and images that mimic real emails from legitimate sources. This is what makes phishing particularly evil. For example, attackers wasted no time in 2020 to use the horrors of the pandemic to their advantage. Emails offering COVID and unemployment assistance were rampant, and many of these emails manipulated groups that typically lack computer literacy, like the elderly.

But phishing doesn't just impact end users. Business email compromise (BEC) has been wreaking havoc for businesses for the past few years.

> *In 2021, BEC accounted for nearly $2.4 billion in losses.*
>
> — FBI IC3 2021 Report

We can see an example of this evolution in phishing campaigns through attacks initialized by APT groups and threat groups in general. These groups target businesses, distributing phishing emails to employee email inboxes.

Like we mentioned in the section above, these emails include malicious attachments, executable files masqueraded as pictures, PDF files with hidden embedded JavaScript, malicious Office documents containing weaponized macros, malicious zip files, HTML files with redirections that download additional malicious payloads, malicious spoofed URLs, and much more.



Then and now

2000

Love Bug: ILOVEYOU

One of the most well-known phishing attacks in history is the “ILOVEYOU” attack, also known as “Love- Bug.”

In the year 2000, victims received an email with the attachment “LOVE-LETTER-FOR-YOU.TXT” as a.txt file (which was really a .VBS file). The file, which had the capabilities of a worm, automatically harvested the user’s Microsoft Outlook address book and sent a copy of the phishing email to all its contacts – spreading itself endlessly. The attack allegedly affected millions of computers around the globe and caused $10 billion in damages.

2021

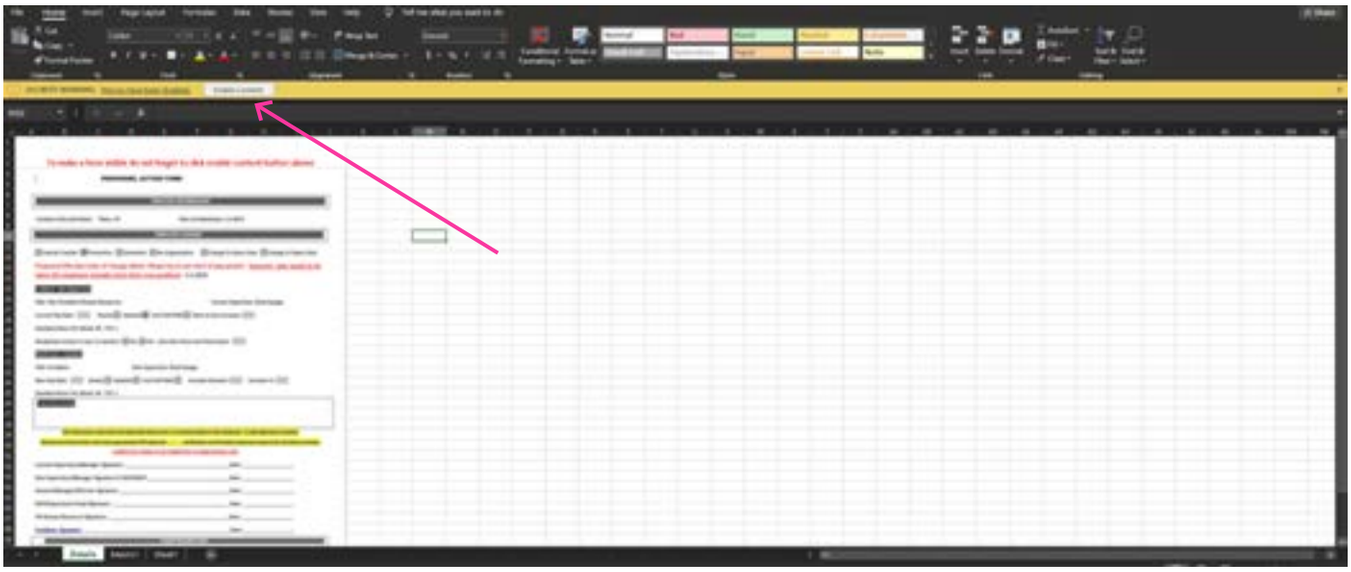
Dridex

Fast forward to today, attackers are investing their time evolving this simple but highly effective tactic. In December 2021, a threat group by the name Evil Corp executed a phishing campaign that spread destructive malware – Dridex.

Dridex specializes in stealing bank credentials. In most cases, initial access takes place via malicious Office documents known as MalDocs, which is an Office document that has weaponized macros. In this recent Dridex campaign, the threat group took advantage of human emotions, innocence, and concerns.

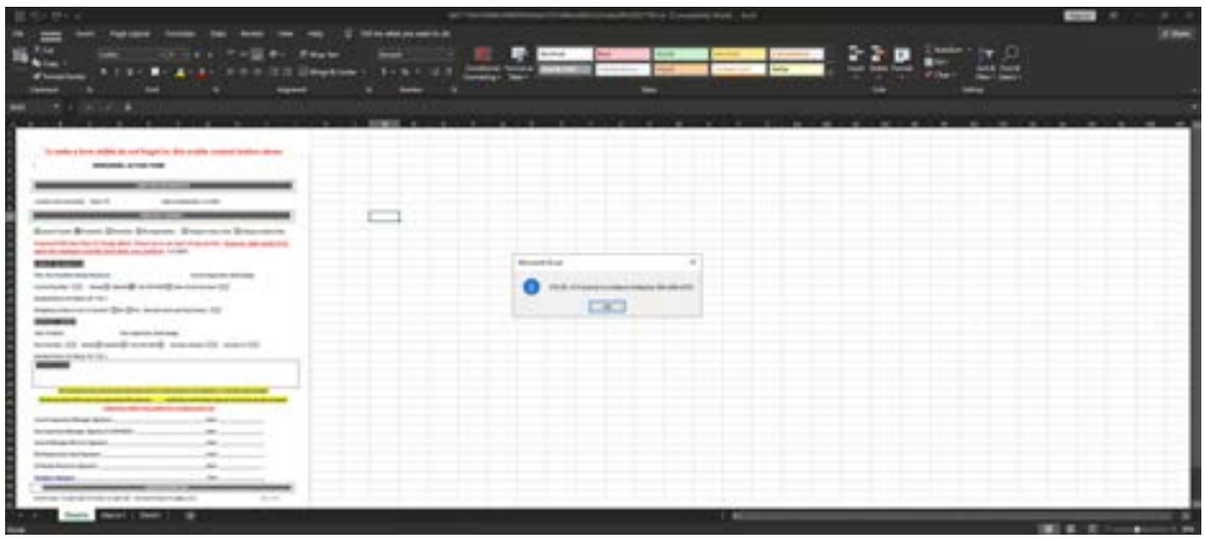
The threat group distributed phishing emails with the subject line “COVID-19 Testing Results.” The email body included an informative letter to the victim, claiming the user had been exposed to a coworker who tested positive for OMICRON (a COVID-19 variant) and guiding the user “to take a look at the details in the attached document.”

The image below is a sample of a weaponized macro Excel file that has been used in the recent “Dridex- OMICRON” campaign.

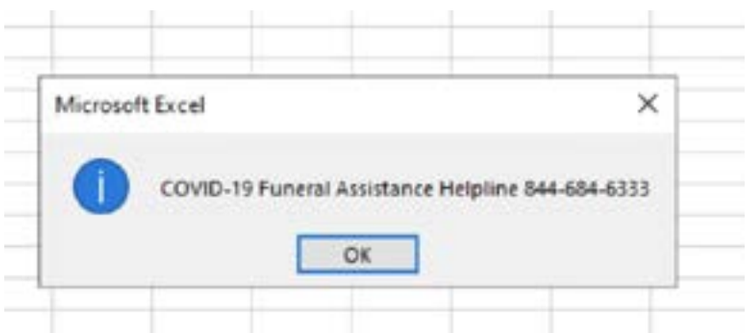


As you can see in the image, the user must click on the “enable content” button to remove the blur from the image and make the “details” visible. When the user clicks on “enable content,” the document runs the weaponized macros that execute the document’s malicious hidden content in the background.

To establish a sense of legitimacy, the Evil Corp threat group added a pop-up message box when clicking on the “enable content” button.



The pop-up message box showed a phone number (844-684-6333). This number is the official number of the “COVID-19 Funeral Assistance” that is supported by the Federal Emergency Management Agency (FEMA). It’s assumed that Evil Corp was geographically targeting American businesses during a time of chaos and confusion.



How to prevent social engineering attacks

As social engineering becomes more sophisticated, it will be more difficult to recognize and prevent attacks. That's why education is critical — companies need to be constantly aware. In this section, we'll review tips, solutions, and approaches for avoiding social engineering attacks.

Adopt an awareness mindset

All of us are constantly exposed to cybersecurity risks. This might sound a bit dramatic, but with awareness and vigilance, the likelihood of being a victim will reduce significantly. This involves educating yourself and keeping your eyes open. You don't have to be paranoid; just maintain a healthy level of skepticism.

If you're on an IT team, make a point to educate your users. And do it often because new tactics and ploys pop up constantly.

It's also important to recognize our vulnerabilities as people. Think about things like curiosity, sympathy, pity, fear, empathy, respect for authority, urgency, and more. These are the things attackers love to prey upon. The key to avoiding these threats is to maintain skepticism, and if something doesn't feel right, listen to your intuition.

Remember, a lot comes down to individuals. To improve the awareness of social engineering in a company and overcome the risks associated with end users, look to your IT and security teams to create and implement social engineering awareness and training. IT teams should also send out regular phishing tests to help their employees develop the muscle to spot a phishing attempt.

Don’t talk to strangers

Remember that saying from when you were a kid? “Stranger danger.” The world, and especially the internet, is a place with many bad actors. If you don’t know someone and they seem suspicious, don’t interact with them.

Stay aware of your surroundings

Threat actors will attempt to enter buildings by acting like they belong there, impersonating an employee by wearing similar clothes, etc. Do you see a new face? Don’t let your doubt stop you from saying something. Ask for an ID, a supervisor’s name, or any other identifying questions. Or verify the person with another employee.

Don’t open emails or texts from unknown senders

Have you received an email or text from a sender you’re not familiar with? Approach with caution. And if you spot a phishing email in your business email inbox, report it to your IT team. That allows them to block the sender and investigate whether other employees have fallen for the ploy. In addition, if you receive an email unexpectedly from your coworkers that includes an unknown URL, attachment, or abnormal request, ask them about it in a different communication channel. Threat actors can spoof an email to look like it’s from an internal resource or user.

Don’t plug in unknown USB devices

Unknown USB drives/devices carry security risks. Threat actors infect them with malicious content (malware) and modify them in order to run the content directly once the flash drives are plugged in. Remember these best practices for USBs:

- Do not plug any randomly found USB drives into endpoints/computers, even if you’re curious about what it contains.
- Report any unknown/unfamiliar USB drives that have been found near your office.
- Set system security policies to disable USB ports on your machine or via the domain group policy.
- Disable the Autorun feature on your machine or company endpoints. Autorun is a feature that allows Windows to automatically run the startup program when a CD, DVD, or USB device is inserted into a drive.
- Ask for approval before plugging in any unknown USB drives/devices.

Level up cybersecurity and company-wide awareness

Companies and organizations should adopt security technology, like endpoint detection and response (EDR), anti-viruses, intrusion prevention systems (IPS), and anti-spam filters. This protects their users from being exposed to malicious content and reduces the risk of attackers gaining access to endpoints.

Social Engineering Toolkit

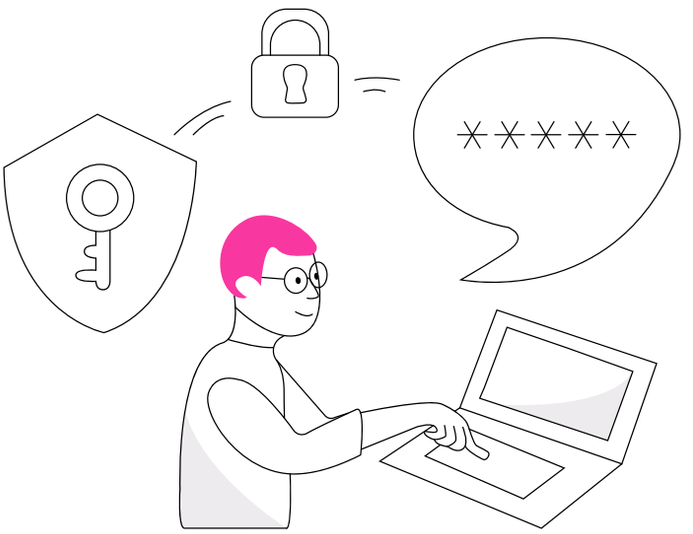
There’s an open-source Python-driven tool for penetration testing. It simulates advanced technological attacks in a social-engineering type environment. The tool generates attacks like: Spear- Phishing Attack Vectors, Website Attack Vectors, Infectious Media Generator, Mass Mailer Attack, Arduino-Based Attack Vector, SMS Spoofing Attack Vector, Wireless Access Point Attack Vector, QRCode Generator Attack Vector, and more.

Get the Social Engineering Toolkit

Next steps

After learning about the world of social engineering indepth, take a moment to ask yourself where you stand. Do you feel prepared to spot a social engineering attack, and if so, do you know what to do when you see one?

Use this white paper to help you shield yourself, your company, and its users from social engineering. And keep in mind, you don't have to go it alone.



Managed detection and response teams

Organizations are increasingly turning to managed detection and response (MDR) providers to ensure their critical assets remain safe. MDR teams are made up of skilled analysts who provide alert monitoring, attack investigation, assistance with incident response, and other services depending on the vendor. For example, some MDR services also include proactive threat hunting and penetration testing.

Note that not all MDR service providers are the same. It's important to find a provider whose capabilities will meet your unique business needs and help you achieve your goals.

Looking for an extra layer of invulnerability?

Some businesses have invested heavily in security technology, creating an unwieldy security stack. Other companies and organizations don't have the budget to invest in an abundance of technology and lack the staff or skills to manage them. And with the way attackers are quickly evolving their tactics – like social engineering – it's nearly impossible for lean security teams to keep up.

The result?

Companies and organizations of all sizes are finding themselves exposed to the storm of threats. And many of these security teams are protecting our vital industries, like healthcare and education. That's why Cynet set out to ensure these organizations have access to the comprehensive cybersecurity they need to stay safe.

A single-solution platform

Cynet's 360 AutoXDR™ end-to-end and natively automated platform integrates with the security technologies you need without requiring the ones you don't. It provides complete visibility into endpoints, users, networks, and SaaS applications, along with extensive automated response capabilities.

And it's backed by a complementary 24/7 MDR service.

Meet the CyOps teamy

CyOps is Cynet's MDR team. They monitor our customers' environments 24/7 and provide guidance from some of the top security practitioners in the industry.

With Cynet's 360 AutoXDR™, you get all this at no extra cost:

24/7 Availability

Ongoing operations at all times, both proactively and on-demand per our customer's specific needs.

Alert Monitoring

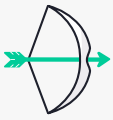
Continuous management of incoming alerts: classify, prioritize, and contact our customer upon validation of an active threat period.

Exclusions, Whitelisting, and Tunnelling

Adjusting Cynet 360 AutoXDR™ alerting mechanisms to our customers' IT environment to reduce false positives and increase accuracy.

Threat Hunting

Proactive search for hidden threats leveraging Cynet 360 AutoXDR™ investigation tools and over 30 threat intelligence feeds.



On Demand Analysis

Customers can send suspicious files to analysis directly from the Cynet 360 AutoXDR™ console and get an immediate verdict.

Attack Investigations

Deep-dive into validated attack bits and bytes to gain the full understanding of scope and impact, providing our customer with updated IoCs.

Remediation Instructions

Conclusion of investigated attacks entails concrete guidance on which endpoints, files, user, and network traffic should be remediated.

We Are One Click Away

CISOs can engage CyOps with a single click on the Cynet Dashboard App upon suspicion of an active breach.

Want to learn more?

Watch our demo to learn how Cynet's 360 AutoxXDR™ platform works.

Check out our CyOps page to discover how our defenders help our customers sleep better at night.