PHISHING TECHNIQUES

Phishing is one of the most widespread and dangerous cyber-attacks today. It targets human mind vulnerabilities thus turning every employee in a potential backdoor to company assets. In phishing, everyone is a target. Not surprising that cybercriminals invent more and more sophisticated phishing techniques day-by-day.

Read about the cutting-edge tricks of phishing attacks – and check your ability to fight them back.

Smishing

Smishing is a kind of phishing conducted via SMS. It's very simple but profitable for the cybercriminals. You may receive an SMS from an unknown girl inviting you for a date with a link to the photos in her profile in a social network. Of course, to see the profile you'll be required to sign in first on the phishing page the link is connected with. Another popular topic of such SMS is "problem with banking account or credit card". In this case, the link goes to a bank phishing page.

In general, the topic of such SMS may be various but the pattern is always the same: to lure users into clicking the link and input their credentials. But there are some additional attack options when it comes to Smishing:

- ✓ Premium SMS: with a reply to the message, a victim may subscribe to a paid service
- ✓ App installation: depending on the OS version & type, the user can be tricked into downloading apps that take control over his/her phone.

Real life example
A typical SMS based attack happened end of 2018, when criminals used SMS phishing to rob cardless ATM's.

OTP bypass phishing

OTP (One-Time-Password) is a part of two-factor authentication that many people use to secure their accounts. Besides the login and password, you need an OTP that is usually sent you by SMS. The process looks super secure, but now cybercriminals have invented the methods to bypass this protection with phishing tricks.

Imagine, you receive an email with a link to your account with two-factor authentication and click on it. Then the real website login page opens, you get the OTP and successfully log in. It seems nothing bad has happened, right? Don't jump to conclusion. Yes, the website you've logged in is not phishing. But, as you click on the link in the email, all your traffic goes via the malicious attacker's server that extracts your cookie and passes it to the attacker. Using that cookie, the attacker can easily impersonate you and log in in your account.

Real life example
Swedish bank Nordea was one of the first victims of a large attack in 2005, when its paper-based OTP security system was infiltrated by a phishing scam. So if OTP phishing is not news, is there any other evolving technique? The quick answer: no. Phishing and social engineering is one of the oldest hacking techniques that exists. That's why we think it is time to give an overview of the different technical attack methods.

Attachment based phishing

Phishing comes to many victims in the guise of a link in an attached file. Very often it’s a .pdf, that contents nothing except the malicious link. If you click on it, you’ll get to a phishing webpage that will try to lure out your credentials.

Nowadays many people are aware that a .pdf can have a poisonous filling inside. But what about other files, for example, voice records .eml? Can they be dangerous?

Just imagine you get a message like “New voice record received” with the attached file. Of course, you are curious to know what is inside – and click on the file. Then a Microsoft Login page downloads and prompts you to enter the credentials. Many people find it logical—as Microsoft care about their security. Bad news for them: the credentials fall right into the cybercriminals hands. Sometimes it could be an HTML file, disguised as web-form from your bank to fill in immediately. In reality, it contains a script to open a phishing page with web-form in your browser. In all cases impact is the same – cybercriminals get your credentials.

Real life example
One of the phishing campaign which is currently underway in 2019, that pretends to be a voicemail received through RingCentral.

Machine learning on the cybercriminals’ service

What if you find in your Gmail a letter from someone you know on the topic you’re interested in with a .pdf in the attachment? Many chances are you click on the attached file, right? Then Google login page will open and ask you to input credentials. It looks trustful, because it even has google.com in the address bar, throughout looking a bit strange, like: “data:text/html,https://accounts.google.com”.

But in reality, nothing is as it seems. The page is phishing, the .pdf is an image with an embedded link and the name of the sender and the topic was picked up from a hacked machine of one of your contacts. How? The malicious algorithm digs into contacts of already hacked machines and automatically creates and send new phishing emails with correspondent names and topics. That’s how the automated spear-phishing with machine learning works.

And that’s not the only instance of ML and AI using by phishers. It also lets them extract plenty of information about the users from the Internet, especially social networks. Earlier, an attacker had to gather information about a victim personally spending a lot of time. Now an algorithm can gather the information and create a spear-phishing email on that base. So, the number of potential victims is growing exponentially.

Real life example
Using the Phishtank database, a group of cybersecurity biz based in Florida, USA, have built DeepPhish, which is machine-learning software that, allegedly, generates phishing URLs that beat defense mechanisms.

Deeplocker is another set of a new breed of highly targeted and evasive attack tools powered by AI. precedent.

QR code phishing

Have you ever used a QR code? Of course, everyone uses it today. But only a narrow circle of security experts aware of the risk of this process. The matter is that everyone can create his own QR code in seconds – including cyber criminals, of course. They can forge a QR code of some trustful organization with URL of their malicious website. So, you can think you input your credentials on your bank website – but in reality, you give them away to the cybercriminals and they empty your account. This attack even more hard to detect, because URL address in QR code is used in short form so you can't check if it's correct before the website is downloaded.

Another cunning attack using a QR code steals credentials from instant messengers like WhatsApp. The attackers use a malicious application that runs a server between the user and WhatsApp web interface. The application opens a real WhatsApp page prompting the victim to log in via QR code. If you do that, the app intercepts your login data on its server and extract them in a text file. And voila – the attacker now can log in into your account, read your messages and impersonate you in correspondence.

Real life example
With the rise of latest trend of using QR Code in Malaysia, China – multiple cases were observed where adversaries were using QR codes to steal both data and money from people.

Vishing (voice pishing)

This type of phishing might be the oldest one – deceiving users to extract secret data via phone dates back in the 1990s. The point is a simple one: scammers call you from "your bank" and try to elicit your account and card data with cunning questions. But nowadays vishing has stepped up a new level. Not only human scammers call victims to lure their credentials but bots and robots as well. This is a real technical leap of cybercriminals because it lets them attack a huge number of potential victims with almost no efforts 24/7. Today bots can impersonate humans very plausibly and this ability is skyrocketing with progress in Machine Learning and AI technologies.

Real life example
Multiple cases of fraudulent communication have been observed wherein, the adversary claims to be from the Canada Revenue Agency (CRA) requesting personal information and in many cases, also using a threatening or coercive language to scare individuals into paying fictitious debt to the adversaries account (which the attacker forges as CRA account).

Phishing Kits

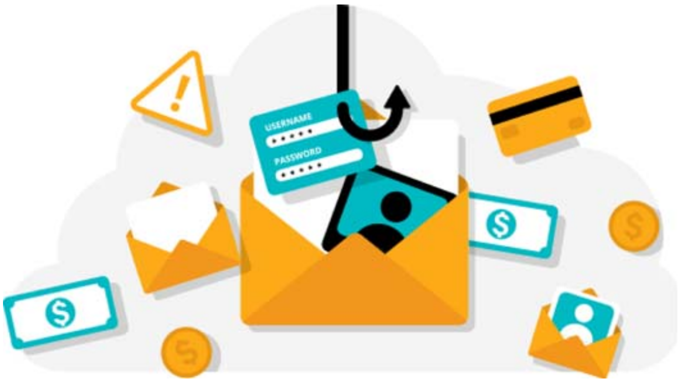
There are many tools for phishing that even non-techy user can easily run. On Darknet, scammers can buy stuff called “multi-brand phishing kit” – a software that let them create a very plausible clone of famous internet- shops. For a scammer, it is enough to deploy such malicious website and advertise it to get the site in the first lines of search engines. Actually, it’s a combination with another kind of phishing – Search Engine phishing. To entice victims, the crooks announce on their sites a “big sales” with unbelievable lower prices for the most popular goods like fancy smartphones and laptops. (They steal pictures and descriptions of the goods from the real online-shops). To buy them, the users are required to input their credit card numbers and other personal data and… you know how sad the story ends.

Real life example
Recently in 2018, a new generation of phishing kit –[A]pache phishing kit, that’s being sold on the Dark Web by a cyber-criminal known as ‘[A]pache’. The software reportedly allows would-be cyber criminals to create realistic-looking fake websites of reputable brands, such as Walmart. The kit is said to be aimed at a Brazilian audience for the most part, but there are some other that also target US brands.

Sextortion

One day you may find a letter in your mailbox beginning with the phrase “You password is…” and containing your real password for some account. Then the attacker intimidates you with a statement that he has hacked you PC and recorded a compromising video of you watching an adult website. Now your computer is under his total control, he says, and if you won’t pay a ransom immediately the video will be sent to all contacts from your address book.

But in reality, all of this is nothing but a bluff. No one hacked your machine. But how the crook had found out your password? It’s not an enigma. He took it from a stolen database of an internet - shop or other web-recourse where you signed up sometime. Such databases are widely sold in Darknet. So all you need to do is to change the stolen password — and forget about it all.



Real life example
Thousands of people all over the world have been receiving sextortion emails from scammers across multiple scams. In a recent sextortion scam, hundreds of military members across US Army, Navy, Air Force and Marine Corps were victims of a scam wherein, prison inmates posing as women developed a relationship online, further sharing sexually explicit photos with the service members. Post sharing pictures, they scammed the service members with demanding money, quickly changing their tone. The scheme stole more than $560,000 from more than 400 military members, as per Naval Criminal Investigative Service.

IDN spoofing phishing attacks

IDN stands for Internationalized Domain Name — domain names written in languages other than English. Correspondently, this attack is based on the fact that some letters in alphabets of many different languages look similar. For example, Cyrillic “n” and “r” looks similar to Latin “h” and “p”. These letters are homographs. So changing some letters in a URL to the similar-looking from another language lets cybercriminals easily spoof a website. For example, if an attacker changes English “p” for Russian homograph “p” in apple.com, he can create a web-domain that looks absolutely the same. More of that, the attacker can even legitimately get an SSL certificate for this site. That means that you’ll see hptts://www.apple.com in your browser’s bar looking exactly the same as the real URL of Apple website and thus give away your credentials to the criminals.

Real life example
Certain exploit kits used the IDN spoofing techniques to distribute the malware. One famous example is the “RIG exploit kit”

Subdomain takeover

Cybercriminals can take over a subdomain of a legitimate company website. How? Imagine, you have a service on a subdomain of your company website. The service is registered on Amazon S3. After a while, you disappoint in the service and quit it, but don’t care about removing the DNS entry connected with Amazon S3 Bucket — a feature that contents subdomain name. And here the cybercriminals come to play. They register this vacant S3 bucket for themselves and use it for malicious purposes like phishing. But as DNS stay linked to your subdomain address, you may be very surprised someday finding out your closed subdomain is alive and serves for criminals.

Real life example
This attack became very popular when an attacker used a subdomain takeover to deface a site used by President Donald Trump for campaign fundraising.

Phishing via web-applications vulnerabilities

Many security flaws in web-applications can be used for phishing. One of them is using a legitimate website with Open Redirect vulnerability. In this case, an attacker can add to the website URL an external link redirecting to a phishing webpage. Most users will notice only the first, legitimate part of the URL – and have a false sense the site is secure.

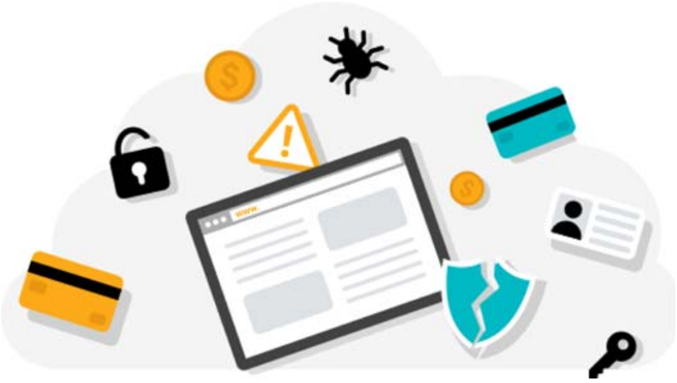
XSS (Cross-Site-Scripting), one of the most popular attacks on web applications also is used for phishing – and not only in one way. For example, an attacker can add a malicious JavaScript to the website URL to redirect users to a phishing page. Exploiting XSS, he also can embed the phishing page right on the website. XSS attacks are also used to provide content injections — one more way to propagate phishing attacks. In this case, malicious data is injected into the legitimate content. As a result, a user sees a phishing element –for example, a faked web-form –on the trusted website and think it's true. Sad outcome is obvious.

Real life example
This type of attack was first registered in 2006 when a vulnerability in PayPal was exploited in a phishing attack. Thousands of similar attacks followed the coming years. Especially those platforms where JavaScript code could be stored permanently (like in an ad or auction) were a great risk for the users. Ebay was one of the top targets in this domain.

Pharming Phishing

This attack redirects legitimate traffic to a phishing webpage right inside your PC. For example, you type in a browser "google.com" but instead get to a phishing website. How is it possible? By changing "hosts" file on your computer with malware that somehow infected your workstation. In this file, the malware set wrong correspondence between IP addresses and a domain name thus redirecting the traffic.

In our example, the malware has changed the real IP address of google.com to the IP address of the attacker's website. Of course, cybercriminals can do it to any domain name, including your bank or social media website. Being unaware, you are redirected to phishing web-page, input your credentials – and troubles begin.



Real life example
There have been occurrences from 2007, wherein in an instance over 50 financial institutions that targeted online customers in the U.S., Europe and Asia-Pacific were shut down due to a large scale Pharming attacks, but not before it was able to infect at least 1,000 PCs per day over a three day period. The targeted companies were Barclays Bank, the Bank of Scotland, PayPal, eBay, Discover Card and American Express.

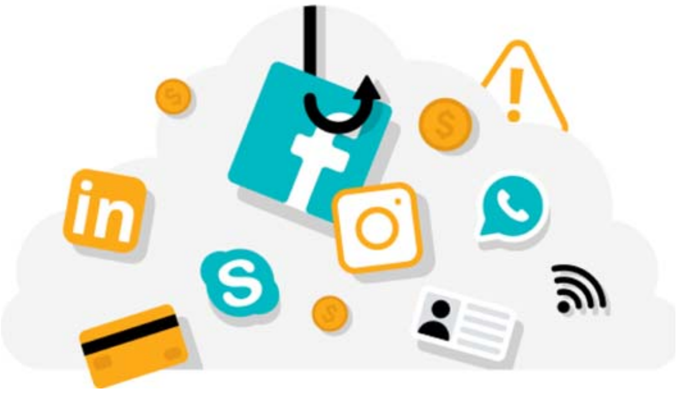
Impersonation or BEC attacks

Business Email Compromise (BEC) attacks are phishing emails that do not have a payload such as a URL or attachment. Instead they use impersonation and knowledge of the company structure or common transactions to convince employees to wire money or data, or to change bank account information for pending payments. As per the latest figures from FBI[1], over the past years (particularly in last 2 years), Business Email Compromise (BEC) schemes have caused at least $3.1 billion in total losses to roughly 22,000 organizations around the world. Ever since January 2015, there has been a 1,300% surge in recognized exposed losses, amounting to an average loss of $140,000 per scam.

Real life example
On January 24, 2018, First Business Bank received a $15,850.00 wire transfer request via email from a business client CEO. The email came from the CEO’s business email address, and the business’s bookkeeper was copied on the email. Our bank employee emailed back a blank wire request form and blank wire agreement to complete the transaction. Soon, a return email came from the CEO’s email that included the completed wire request form and wire agreement, both of which also had the CEO’s authentic signature.

Phishing via Social Media

As with Smishing, these attack vectors (for instance malicious links, impersonation etc.), gets delivered through the new breed of social media collaboration apps for instance (Whatsapp, LinkedIn, Slack, Skype, Teams, Facebook Messenger). While users have been trained to be suspicious of email, they tend to be overly trusting when using these tools.



Real life example
In 2017 Facebook disclosed that up to 270 million accounts were illegitimate while Twitter identified over 70 million fake and suspicious accounts in 2018. As per the report from Corrate, most of these accounts were used for spreading phishing via social media via nefarious use of the platform.