What Is Phishing and How Can You Avoid It?

By Pablo López-Aguilar Beltrán, Head of Cybersecurity, APWG.eu

Cybercrime is, nowadays, one of the biggest threats faced by Governments, industries, and the society as a whole. In fact, the global loss caused by cybercriminals throughout 2020 amounted to 5.5 trillion euros[1]. Far from decreasing, it is more than likely that this amount will increase in the coming years.

Cybercriminals use a myriad of techniques to circumvent security measures, but the truth is that, at the end of the day, the human factor offers them an *easy* and cost-effective way to achieve their goals. The unprecedented situation brought by the pandemic has added to this, not only because of the extra time we are spending on the Internet but also because of the increased amount of people suffering from anxiety.

This new paradigm provides an open window for cybercriminals, who now see endless opportunities to commit their fraudulent activities under the feeling of protection[2] of the Internet. **Phishing**, a technique where a victim receives an email[3] impersonating a legitimate source and is pushed to click on a specific link, is the best known of them. Clicking on that link can have devastating consequences, including personal or confidential data thefts, malicious software (malware) downloads or unauthorized accesses to a company's network[4].

Features of a phishing attack

The success of phishing attacks is attributable to the use of social engineering techniques to gain the trust of a victim. As said before, the most common method starts when the victim receives an email that appears to be genuine. These emails can be sent either indiscriminately or with specific targets (spear phishing).

While phishing attacks can vary widely, cybercriminals tend to follow a number of very common patterns.

First of all, they collect information on their victims thanks to publicly available information on the Internet (on social media, search engines or by using tools such as Maltego, Pipl…).

[1] The EU's Cybersecurity Strategy in the Digital Decade: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

[2] It is relatively difficult for law enforcement agencies to present evidence of crimes committed on the Internet in court. This is why the European Union is investing in projects like LOCARD (https://locard.eu), aimed at enabling law enforcement agencies to process digital evidence by blockchain and to generate mutual recognition of sentences across different courts of justice in the EU.

[3] There is some controversy on this point. Whereas some experts define *phishing* as a technique that exclusively uses e-mail as an attack vector, others define it as a technique that, in addition to e-mail, also uses the telephone or text messages as attack vectors. However, while terms such as *vishing* or *smishing* are used to refer to the two attack vectors mentioned above, there is currently no term to define phishing attacks produced exclusively via email. Should we maybe invent it? Something like *mailshing*?

[4] According to the latest report from the Anti-Phishing Working Group (APWG), phishing attacks doubled in 2020: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf.

Based on the information collected, they create their *scenario* (also known as *pretext*), that is, the message intended to generate credibility for the victim.

Once the pretext is defined, they decide on the attack vector to send the message. The pretext message is usually sent by email, phone or text message (or even a combination of all three vectors).

Finally, if the attack is successful, they will put the stolen information for sale on the Dark Web, they will extort the victim by requesting a sum of money either to have it back or to unblock it (ransomware) or they will use it to gain access to the victim's company's internal systems. If unsuccessful, they will probably follow the same pattern again, but with an improved pretext.

How to prevent phishing

In order to prevent a phishing attack, it is important to understand that its basic principle is building credibility. In that respect, social psychologists differentiate between two forms of processing information—systematic and heuristic.

Systematic information processing takes place when, using some piece of information received, we make a decision in a rational manner, analyzing all details carefully (sender, contents…). On the contrary, when processing information heuristically, we use mental shortcuts to make decisions. We operate in the systematic mode when the information we are processing is important. However, factors such as time pressure, distractions, or emotions can make us switch to heuristic information processing[5].

Consequently, in their phishing attacks, social engineers will try to build credibility and have their victims operate in the heuristic processing mode, for instance, by engaging them in a phone call where they are asked to solve some urgent matter or, taking advantage of the current situation, by sending them an email encouraging them to purchase pandemic vaccines. In both pretexts, the fraudsters will always attempt to impersonate the identity of a known sender in order to generate credibility.

Some tools can be very useful to help us prevent these types of attacks[6]. However, the following list of recommended good practices, when properly applied, could help to significantly reduce the success of most phishing attacks. None of them require any technical expertise, just common sense:

- Verify and double check the identities of senders by asking questions or doing some Internet research. Never click on a link from a sender that has not been verified before.

- Never give personal details via email or on the phone if you are not certain about the sender's real identity.

[5] This behavior is described in detail in the book *The Art of Deception*, by Kevin D. Mitnick and William L. Simon.
[6] Tools such as DMARC allow for very effective filtering of potentially fraudulent emails: https://www.globalcyberalliance.org/dmarc.

- As staff members of a company, learn how to offer resistance to social engineering and modify your email courtesy rules. To say it differently, it would be advisable to put sender verification policies and processes in place for all corporate email (especially for those cases where a sender pretends to be an executive of the organization).

- Keep all software installed on your electronic devices up to date.

Finally, it is worth noting that the massive use of electronic devices, together with the anxiety caused by the pandemic, have laid the ideal foundations for cybercriminals to achieve their goals. Despite the effectiveness of many tools, the human factor is still seen from a very generic point of view, which usually disregards specific psychological aspects that could have an impact on the victims' susceptibility to social engineering attacks. Therefore, it is important that governments and companies join forces and develop defense strategies based on improving the psychological understanding of the human factor.

Because, in an increasingly digitalized world, we—the people—are the new perimeter of defense and, undoubtedly, the first protective wall against cybercrime.