Phishing: what it is, how to prevent it and how to respond to an attack

By Nicola Tacconi, CISO Aruba S.p.A.

Phishing is a scam conveyed via the Internet, where attackers try to deceive their victims in order to gain access to sensitive information such as usernames, passwords or bank details. Generally, the cyber criminal sends false communications to the victim, posing as a well-known company, or as someone with whom it is possible to have conversations and relationships, using plausible excuses to obtain the victim's personal data.

The phenomenon of phishing is a current and frequent threat. In its latest report, Kaspersky Lab has revealed a two-fold increase in the number of attacks blocked, with 44 per cent of attacks detected aimed at banks, payment systems and online shops.

So, how can you spot an attack? Phishing usually presents itself as a digital communication that reaches the recipient via email, SMS, a social network or on the user's main Instant Messaging platforms. Phishing attacks generally share one or more of the following features:

- communication of a suspension or blocking of an account without explanation;
- a request for payment linked to a specific transaction by a fictitious expiry date;
- the presence of a web address that includes a similar domain but is subtly different from the entity's legitimate address;
- a request for private information;
- misspellings in the message body.

There are a series of measures that allow you to navigate the online world more safely and minimise the risk of falling victim to the attack, including:

- **Keeping your browser up to date**. By installing the latest versions of software and inserting anti-spam filters, or special plug-ins, the browser will be able to prevent a greater number of phishing attempts;

- **Checking the domain from which the communication originates**. A company or an entity will always write from its own domain, so you should always check that it corresponds to the official one. This verification does not provide a complete guarantee of authenticity, but represents an important first check that can be carried out;

- **Being careful not to click on the links in the emails**. As a good rule, it is advisable to never click on the links contained in the communication, but to instead type the address of the official site of the sender directly into the browser and to verify directly on the site the content described in the email;

- **Using multiple email addresses.** When you subscribe to services or websites of dubious reliability, it is preferable to use secondary emails, so as not to risk contaminating your main email inbox;

- **Contacting customer service**. If an ambiguous email arrives and it is not clear whether it is a fraud or not, it is always safer to contact the customer service of the company to which the email refers;

- **Reporting a phishing site to help other users avoid scams**. Each report is useful in highlighting a warning message about the potentially dangerous site. Reports can be sent, for example, through PhishTank, Google Safe Browsing or Microsoft Smart Screen;

- **Using secure email services.** It is advisable to use professional email services, equipped with security protocols such as SPF and DMARC on incoming (and outgoing) mail.

However, if you or one of your employees happens to fall into the trap, there are a series of actions that should quickly be performed so as to limit the damage:

- **Change your password.** In the case of online portals, you must change your password or close the profile directly before hackers can access it;
- **Contact customer service**. If the account has already been compromised and it is no longer possible to log in with your data, you must contact customer service to manually restore your access data;
- **Contact your bank in the event of theft of bank data**. The credit institution must be contacted to block the financial services involved in the scam (credit cards, current accounts, debit cards and more);
- **Alert the affected institutions**. In addition to the recovery of personal data, it is advisable to report the phishing attack to the bodies that have been affected, so that they can take measures to counter the scam.

Phishing, even though it may seem like nothing more than a deceptive email, is a real crime, and as such should be treated as one. This is why the next step of any reported attack should be to inform the revelant authorities. Although it is not required by criminal law, phishing is nowadays judged as computer fraud and digital identity theft. Furthermore, as a computer crime, it is necessary to notify Action Fraud, which has a designated space on its website for such reports.

In conclusion, there are a great deal of phishing attacks out there but, thanks to the various countermeasures that can be taken, the percentage of intercepted, blocked and unsuccessful attacks exceeds 80%. The remaining 20% of attacks require a conscious collaboration between service providers and customers. By carefully reading the emails you receive, only entering your data into reliable sites and avoiding opening suspicious links, phishing is a problem that can be avoided.

Aruba S.p.A.

Aruba SpA, founded in 1994, is the first company in Italy for Data Center, cloud, web hosting, e-mail, PEC and domain registration services and has extensive experience in the creation and management of Data Centers, having a network active at European level: in addition to proprietary Data Centers - 3 already active in Italy and one arriving by 2020, plus another in the Czech Republic - additional partner structures are in France, Germany, UK and Poland. The company manages over 2.6 million domains, more than 8.6 million email accounts, over 6 million PEC accounts, over 130,000 servers and a total of 5 million customers. It is active on the main European markets such as France, England and Germany and boasts leadership in the Czech and Slovak Republics and a consolidated presence in Poland and Hungary. In addition to web hosting services, it also provides dedicated server services, housing and colocation, managed services, digital signatures, substitutive conservation and smart-card production. Since 2011 it has expanded its offer with Cloud services and in 2014 it became the official Register of the prestigious "cloud" extension. Aruba Data Centers can host over 200,000 servers. For further information: https://www.aruba.it.

Red Lorry Yellow Lorry

Ghislain d'Andlau/Emma Davies

Email: aruba@rlyl.com