INTERACTIVE SESSION MANAGEMENT

Phishing for Money: Dangerous Emails

In 2018, the Dutch branch of Pathé received an email from the cinema conglomerate's headquarters in France. A manager at the French office told the Dutch director and her chief financial officer that there were plans to buy a company in Dubai. Would they transfer the necessary funds? The email certainly looked legitimate. The two Dutch managers made the payment. And again, and again. All in all, they sent $21.7 million. Sadly, the money only ended up in the pockets of digital con artists.

This is an example of "phishing," whereby criminals angle for personal information that they can use for their scams. There are several ways to classify phishing, but a distinction is often made between spear phishing and bulk phishing. The former relates to a phishing attack that is specifically directed at one or two persons—in our example, the director and chief financial officer of Pathé. It would be easy to dismiss these two officials as just exceedingly careless, but in reality, the situation is often more complicated. Many of those who perpetrate phishing attacks do their homework before sending their emails. They often hack the website of the company concerned and study the activity and emails in its system to find out how to make an email more credible. The really dedicated ones even study the writing style of the CEO.

Instances of CEO fraud are not publicly known, but they can potentially be very successful, according to Ken Bagnall, the head of FireEye, a company that focuses on securing emails. He points to the "CEO fraud test" that was sent to a number of companies. The result was stunning: 90 percent of the companies contacted took the bait. Given this success rate, it may seem surprising that few successful attacks are reported in the news, but it is likely that many go unreported. Data hacks have very negative effects on the reputation of companies; clients trust them less and may take their business elsewhere. Companies are more likely to cut their losses rather than report the fraud to the police. If a phishing attack is successful, the long-term damage to a company may be difficult to quantify, but it is almost certainly huge.

In the other type of phishing—bulk phishing—emails are sent to thousands, sometimes even millions of people. Many of these emails are easily recognizable as fraudulent; they often, for instance, contain basic language errors. Sometimes, however, even bulk emails look surprisingly professional.

In 2018, Dashlane, a company that specializes in the protection of passwords, compiled some disturbing statistical data regarding phishing and its incidence. In 2017, phishing attacks increased by 65 percent. According to the company, 30 percent of phishing messages are opened by the recipients, and 12 percent of those recipients click on the malicious link included in the message. In addition, almost 1.5 million new malicious sites related to phishing are being created every month.

The big problem is that phishing has become much more professional as well as cheaper. Most links in the phishing emails are to malicious websites that may replicate the website of an actual bank. For instance, Dutch state broadcaster NOS discovered in 2018 that a Russian site called Boris was selling fake copies of a Dutch bank's website for only $296.

What can companies and individuals do to protect themselves against phishing attacks? The first answer to that question is very simple: be cautious. Even today, phishing emails contain telltale mistakes in grammar. A threat or warning is also a sign that things something is amiss; in such instances, banks advise customers to call in just to check if the email was really sent by the bank.

The second answer is to use security software and ensure that it is updated regularly. Antivirus software programs typically include a list of suspicious websites. Once the recipient of a phishing email is directed toward a malicious site, the antivirus will block it.

Some security experts suggest a third and more extreme answer: make sure that emails never have attachments. Phishing emails often rely on them to make sure that the scam is successful, so in theory this is a good precaution; unfortunately, in practice, it is virtually impossible to send out emails without attachments.

However, even if all possible measures are taken, phishing emails may yet be successful, and it only takes one to cause real trouble for the company. Ken Bagnall, the CEO of The Email Laundry, highlights the dangerous situation that is created once the email account of a CEO is hacked: cybercriminals could then send out emails with every appearance of being the real thing, potentially doing enormous damage.

Sources: "Pathé Verliest 19 Miljoen Door Ceo-Fraude," Avrotros, November 12, 2018, https://opgelicht.avrotros.nl/nieuws/item/13929/, accessed January 12, 2019; "OUCH! Newsletter: CEO Fraud," SANS Security Awareness, July 2016, https://www.sans.org/security-awareness-training/ouch-newsletter/2016/ceo-fraud; Eleanor Dallaway, "#ISC2CongressEMEA: Why CEO Fraud Works and How to Stop It," Infosecurity Magazine, October 19, 2016, https://www.infosecurity-magazine.com/news/isc2congressemea-ceo-fraud/; Eitan Katz, "Phishing Statistics: What Every Business Needs to Know," Dashlane, January 17, 2018, https://blog.dashlane.com/phishing-statistics/; Joost Schellevis, "'Boris' Verkoopt Nagemaakte Nederlandse Banksites Voor 262 Euro," NOS, November 25, 2018, https://nos.nl/artikel/2260826-boris-verkoopt-nagemaakte-nederlandse-banksites-voor-262-euro.html, accessed January 12, 2019.

CASE STUDY QUESTIONS

1. Explain the difference between spear phishing and bulk phishing. Which of the two forms of phishing do you think is most difficult to spot by victims, and why?
2. The CEO of your company received a fraudulent email and made a payment to digital criminals. He wonders now whether he should contact the police. What factors should he take into consideration before taking a decision?
3. Dashlane advises clients to send emails without attachments. Do you think that not adding attachments to emails will help protect companies against phishing stacks?
4. Give two pieces of advice to a company or individual on increasing protection against a phishing attack.

Case contributed by Bernard Bouwman

Cloud computing is highly distributed. Cloud applications reside in large remote data centers and server farms that supply business services and data management for multiple corporate clients. To save money and keep costs low, cloud computing providers often distribute work to data centers around the globe where work can be accomplished most efficiently. When you use the cloud, you may not know precisely where your data are being hosted.

Virtually all cloud providers use encryption to secure the data they handle while the data are being transmitted. However, if the data are stored on devices that also store other companies' data, it's important to ensure that these stored data are encrypted as well. DDoS attacks are especially harmful because they render cloud services unavailable to legitimate customers.

Companies expect their systems to be running 24/7. Cloud providers still experience occasional outages, but their reliability has increased to the point where a number of large companies are using cloud services for part of their IT infrastructures. Most keep their critical systems in-house or in private clouds.

Cloud users need to confirm that regardless of where their data are stored, they are protected at a level that meets their corporate requirements. They