Oh no, I have been sending phishing mails!

In the first place, what is phishing?

Phishing is an invented word cobbled out of the two words “password” and “fishing”. Criminals use fake emails to try to obtain personal data – in particular login data – from their victims by luring them to fake websites and tricking them into entering their data. In the meantime, a multitude of bogus companies exist. For some time now, not only banks, but also online shops, social media, online games, and many more companies are being counterfeited.

Why this article?

A wealth of information may exist for end users on how to recognize phishing (e.g. at https://wiki.botfrei.de/Phishing and https://blog.botfrei.de/?s=phishing), whilst in the meantime, mailbox providers employ standard best practices which allow them to detect incoming phishing emails to the greatest possible extent (e.g. https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf). On the sender’s side, however, the focus is on making their own legitimate emails distinguishable from phishing emails by means of authentication measures – i. e. SPF, DKIM and DMARC – in order to make it easier for mailbox providers to filter out phishing emails.

Unfortunately, it is not inconceivable that criminals might abuse the mailing platforms of professional senders to send phishing emails. This is particularly insidious given that professional senders generally have high-performance mailing platforms and have implemented standard authentication measures. How can you avoid this as a sender and, if it happens, minimize any subsequent damages?

How do I prevent outgoing phishing emails?

A first step which must definitely be taken is the installation of a spam filter at the sender's site, which checks outgoing emails before sending them and automatically stops them if necessary. This filter can also conduct somewhat more “aggressive” filtering than a typical incoming filter for mailbox providers, because in case of doubt, an email can be released after a short delay and only sent after a manual check by an employee.

In addition, it can be helpful to check all links in the emails against standard lists such as the Google Safe Browsing List (https://developers.google.com/safe-browsing/v4/lists) or the PhishTank list (https://www.phishtank.com/). Here too, the transmission would have to be initially halted and checked by an employee. Especially in instances where phishing cases have already occurred on your own platform in the past, you can also derive typical behavior patterns of criminals (user name, login location, login times, payment data, etc.) from the historical data and monitor your own platform for such behavior patterns among the currently active users.

In spite of everything, it still happened; so, what should I do now?

Detecting phishing emails is not easy. Filters and lists are often only effective when something has already happened. Time is of the essence here. The sooner the sending of emails can be stopped, the fewer hazardous emails reach the mailbox provider and thus the end user. Cutting back on the sending speed for new accounts can therefore be a means to extend the reaction time. Continuous monitoring of blacklists, reputation data, feedback loops, etc. helps to detect a case as early as possible and to stop the delivery.

In addition, all redirects (tracking links) contained in the email detected as phishing should be immediately deactivated or redirected to a corresponding warning page. Again, a fast reaction time is crucial! The emails already sent cannot be retrieved, but a phishing victim can be spared further damage if the links in a phishing email do not lead to a malicious website.

Another option for warning the recipients of phishing emails arises in instances where logos and graphics are stored on the sender's computer via a content management system and are loaded by the recipient of the email when it is opened. Here, it is possible to exchange these graphics and mark them with clear warnings that the email is fraudulent. For the end user, there is a big difference between opening a fake email that looks deceptively real or a fake email that looks completely different and which is marked with eye-catching alerts.

Summary

Phishing is a serious problem, and one which – even in times of authentication with SPF, DKIM, and DMARC – is still not resolved. Detecting outgoing phishing emails is not easy, but it is possible. In particular, the comparison with typical behavioral patterns is promising. But even if your own platform has been misused to send phishing, there is still a lot you can do to protect the end user. First and foremost, the quick deactivation or redirection of tracking links helps to minimize the damage caused.

Authors: Technical Team of the Certified Senders Alliance