Phishing-Awareness Specialists: Stewarding Trust in a Digital World

Written by Joshua Bucheli, AI Ethics Researcher and Fellow at the ForHumanity Center, in Collaboration with IT Security Manager Kai Dorner and Peter Kosel, Founder of cyberunity

Illustration from Insta: the_doodling_crow

Over the past couple of years, YouTubers like kitboga and Jim Browning have pioneered an online fascination with exposing call-center scams, a pastime that has become known as 'scambaiting'. Posing as vulnerable IT users, these cyber-vigilantes lure in bad-actors who masquerade as IT support, turning the tables on their phishing scams, exposing them and garnering millions of views in the process.

While comical, what these viral videos highlight is no laughing matter – they show just how easy it is to fall prey to phishing scams, and they demonstrate the crucial need for increased awareness of how to identify trustworthy parties.

Trust is the keystone upon which all of our social, and indeed digital, interactions are based. We trust E-banking with our finances, apps with our passwords, systems with our infrastructures, and clouds with our data. 'Phishing' attacks are a form of social engineering that *preys* on this trust, therefore posing one of the greatest threats to data security.

Where Does Phishing Stand Today?

Unlike cyberattacks that take a brute force approach to cracking encryptions, phishing is a more subtle affair operating on much the same principles as literal angling: you throw out some bait and wait to see who bites. The object is to 'phish' for user data or for access to systems by mimicking a legitimate site. Thanks to its reliance on the simple principle of deception, it has become a staple in the arsenal of cybercriminals the world over.

"Hackers will either coax users onto a faked login page and bait them into entering their sensitive data or trick them into clicking links that download malware or ransomware onto their devices. Such attacks can not only grant hackers access to a system or sensitive information, they can also lock someone out of said systems and data until a ransom is paid." – explains IT Security Manager, Kai Dorner.

What makes phishing unique among cyberattacks is its reliance on social engineering – the manipulation of social psychology – to exploit people.

Anyone interested in more details about social engineering is invited to check out Kai's Anti-Phishing Model, read up on the six principles of persuasion in pages 8-10 of his Thesis, or to hear more about the intricacies of 'hacking humans' here.

Where is Phishing Headed?

As comedian and director Jordan Peele's Obama deepfake demonstrates, the advent of increasingly advanced face and voice recognition technologies is bringing the sophistication of phishing attacks to new heights. As these technologies advance, judging the trustworthiness of content will become increasingly challenging, making 'vishing' (voice phishing) and other variations of phishing all the more dangerous.

Corporations are beginning to catch on to the fact that such issues warrant their attention. However, there is a difference between knowledge and awareness, and for now, awareness of what phishing entails is still limited – the ruinous sentiment 'why should anyone be interested in me?' still proving all too prevalent.

While some sectors, most notably finance, are ahead of the pack when it comes to implementing anti-phishing strategies, overall, most companies still have a ways to go in recognizing the value that even small steps like employee workshops or mini awareness campaigns will bring them in terms of reputation and job security, argues Kai.

"Turning a blind eye is still far too common and it is the worst thing a company can do in this day and age. Even something as simple as bringing up the matter over coffee with colleagues can yield worthwhile results – after all, a dynamic exchange of ideas can be more effective than relying entirely on web-based trainings."

Phishing Specialists – Hard Skills and Qualifications

Phishing attacks exploit trust – protecting against such attacks will therefore, first and foremost, be a matter of raising awareness. Companies will increasingly need CISOs, ISOs, and Operational Risk Officers who can help them differentiate between legitimate and malicious third parties and who, in the spirit of ICS, can train their employees to do so as well.

This entails cybersecurity aspirants with solid analytical skills, a broad combination of IT, cybersecurity, and fraud detection know-how, and the ability to convey these skills to colleagues.

“Employers depend upon individuals who understand how servers are constructed, operated and maintained as well as how mail-filters detect suspected phishing attacks – individuals with solid foundations in network-engineering and cloud- and systems-architecture”, advises Kai.

The larger the company, the higher the likelihood that it will be looking to handle these issues on a more comprehensive in-house basis. For those interested in such positions, large corporations are a good place to look for jobs. In most other cases, consulting is the name of the game, with security consultancies offering more specialized roles in different niches of phishing awareness and cybersecurity.

Practical experience in the implementation of phishing related cybersecurity strategies like multi-factor authentication, VPN and proxy-services, firewalls, data encryption, adjusting filters, and the carrying out of vulnerability analyses and penetration testing are further skills that phishing awareness specialists should emphasise in their applications.

In terms of certificates, any professional training that evidences proficiency in fraud detection, ethical hacking, or cybersecurity in general, such as CISSP, CISM, CCAP, CEH, and Cofense’s PhishMe Certification will be of added value.

Familiarity with international implementation standards and guidelines like the NIST frameworks, the BSI IT-Grundschutz Compendium, the ISACA’s COBIT framework, the (ISC)^2 Body of Knowledge, the MITRE ATT&CK Enterprise framework, or ISO/IEC 27001 will also be an advantage.

All said however, Kai stresses that practical experience is far more valuable than any certificate – “the doors to a career in phishing awareness are open to practically anyone who can demonstrate a passion for and pertinent experience in the issue”.

Beyond Technical Know-How:

As with most other cybersecurity career paths, hard skills are not the only ingredients in the recipe for success. It takes a particular kind of personality to be an effective phishing awareness specialist.

Companies need highly social, ‘awareness-types’ with a knack for spreading a message – team players with the curiosity, patience, and communication skills necessary to handle cases of conflict productively. Ideally, these individuals will also bring with them habits akin to those of security scouts – an eagerness to continuously develop their skills so as to keep up with the ever-evolving world of tech.

Kai rounds off his account of essential soft-skills with the following words of advice: “In the field of awareness campaigning, the ability to put yourself in someone else’s shoes is vital in order to ensure that knowledge is not only conveyed but actually internalised – *empathy* will therefore be one of the most powerful tools in an effective phishing awareness specialist’s repertoire.”

Peter Kosel, Founder, Talent Community Manager, and pioneer of the KNOW YOUR TALENTS recruitment approach at cyberunity summarizes the matter as follows:

“We must take the utmost care not to let this new concern with cybersecurity turn into an obsession. Being overprotective can become a hindrance to good business, and this does no one any good. Letting fear get the better of us would lead us to switch off all our devices – then everything would be safe but pretty much everyone would be out of a job. The trick lies in approaching the question of phishing awareness in a way that is both beneficial to businesses and seen by customers and employees as a sustainable and existentially vital added value – something that will only happen if employers recognize the importance of building and maintaining relationships with experienced individuals: Cyber Security means: KNOW YOUR PEOPLE.”