Opinion Article

This is (not) a drill

How Cofense™ simulations play a key role in preparing your people against the threat of corporate phishing

JOHANNESBURG – October 23, 2018 – Over the past few years, phishing attacks that target us at work have grown in sophistication and credibility. While they still pop up every now and then, the days of badly written e-mails claiming to be from long-lost uncles with millions of dollars merely needing to be 'unlocked' are mostly gone. While these may have been largely resigned to the scrap heap of internet memes, a far more dangerous genre of phishing has emerged.

Today, we're seeing corporate domains being compromised, and e-mails being spoofed from company execs, from suppliers, customers and others. Unwitting junior employees receive seemingly legitimate requests from their CFO, demanding they release funds or change bank account details. HR teams are innocently revealing sensitive personal information based on spoofed requests from their seniors. There are thousands of ways that data and money can be lost – or should we say, 'stolen'.

Advanced phishing techniques in the corporate world are a dangerous phenomenon, says Anton Jacobsz, managing director of Networks Unlimited, which delivers award-winning Cofense™ phishing defence solutions to the local market. It’s causing many organisations to rethink the way they handle the threat of phishing, and how this fits into their broader cyber-security defences.

“Companies are realising that they can’t simply prevent their employees from using communication tools, social media and e-mail to engage with each other and with other players,” notes Jacobsz. “The goal now is to empower employees with knowledge, helping them become more savvy and aware of the evolving threat landscape.”

Step 1: Baseline assessments

Cofense has developed a tried-and-tested array of solutions that do just this: transforming employees from points of weakness into proactive, vigilant armies that look out for every potential threat. In a recent “Left of Breach” e-book, Cofense helps organisations defend against phishing threats using three key steps.

“We essentially take a three-phase approach,” explains John “Lex” Robinson, anti-phishing strategist at Cofense. “We start with a baseline assessment that seeks to understand your current risk exposure. Where are your current phishing weaknesses, as an organisation? What are you doing today to combat the scourge of phishing attempts by threat actors? From there, we identify phishing weaknesses in the organisation and then conclude with getting everyone in the organisation, regardless of title or job role, to report real phishing threats to your incident response teams.”

Robinson says that some of the most important aspects of this initial baseline audit include getting a clear view on:

- Where your most important data is stored;
- Which individuals and groups have access to this data;
- What operating systems, e-mail clients and browsers staff are using;
- Who are the most likely targets of tactics like ‘spear phishing, whaling and spoofing’;
- Which types of phishing attacks are you experiencing today;
- Which employees are empowered to send e-mails with customer data or other high-risk, sensitive information;
- Which corporate systems are able to generate e-mails with customer or sensitive data;
- What are the social media policies and permissions in place; and
- How are employees interacting with third party vendors, consultants, contractors, partners and so on?

Answering these questions helps to build a complete picture, which is then overlaid with a deep understanding of the current phishing landscape:

What are the latest corporate phishing tactics? Which companies have recently suffered phishing attacks? What have been the actions of regulators and law enforcement? How are new innovations like blockchain shaping the ‘black market’ for unscrupulous players? What trends are happening specifically in your industry?

Step 2: Starting the simulations

In the second step, you'll design a series of simulations that serve to mirror real-life attacks. But a word of caution: don't start the simulations too abruptly. To get a fair assessment, you'll need to prepare your employees to some extent.

Cofense best practices indicate that you should announce the programme and its intentions so your end-users understand the intended outcomes, such as learning to recognise and report real phishing threats. While they don't need to be notified prior to each simulation being sent, awareness and understanding from your employees are key components to the necessary buy-in to make your phishing defence programme a success. Additionally, you can start spreading phishing awareness messages through company communication channels, advertising the ways that employees can report phishing tactics.

As you move into the simulation, Jacobsz advises IT security teams to try a broad range of different tactics based on what types of real phishing attacks your SOC is seeing happening within your network, which could range from innocent e-greeting cards, to fake invoice attachments, invitations, links to 'new company policies', statements from the company on current events, or other attention-grabbing messages.

"Overall, this must be done from the perspective of being constructive and helpful to employees. It shouldn't become a witch hunting exercise where the employees who fall for the simulations receive any form of disciplinary action. In fact, the individuals who are most vulnerable to threats need to be given special attention and care," says Jacobsz.

Step 3: Building a sustainable advantage

In the third step, you're able to start constructing phishing awareness messaging that's tailored to your users' needs and to their level of understanding.

Anonymise and publish the results of your simulations; reiterate the ways that employees can report phishing attacks; and conduct further rounds of testing that steadily increase in sophistication.

"It's important to remember that these simulations fit alongside a number of other interventions, such as learner management tools, incident report management systems and management reports," Jacobsz explains.

"When used together, they enable CIOs and CSOs to better orchestrate their phishing defence strategies.

"Simulations play a key role in guiding your employees to become more alert to the threat of phishing, business e-mail compromise and related attacks like ransomware. With empowered, knowledgeable staff, organisations can dramatically shorten the time to detect and respond to attacks - helping to reduce the impact and keep the organisation safe," he concludes.

To learn more about Cofense's phishing incident solutions, please visit: https://Cofense.com/.

About Networks Unlimited Africa

Networks Unlimited Africa is a value-added distributor, offering the best and latest solutions within the converged technology, data centre, networking, and security landscapes. The company distributes best-of-breed products, including Attivo Networks, Cofense, Carbon Black, Fortinet, F5, Hypergrid, Mellanox Technologies, NETSCOUT, NETSCOUT Arbor, ProLabs, RSA, Rubrik, SevOne, Silver Peak, Thales and Uplogix. The product portfolio provides solutions from the edge to the data centre, and addresses key areas such as cloud networking and integration, WAN optimisation, application performance management, application delivery networking, Wi-Fi-, mobile- and networking security, load balancing, data centre in-a-box, and storage for virtual machines.

Since its formation in 1994, Networks Unlimited Africa has continually adapted to today's progressively competitive and evolving marketplace, and has reaped the benefits by being a leading value-added distributor (VAD) within the Sub-Saharan Africa market.

About Cofense™

Cofense™, formerly PhishMe®, is the leading provider of human-driven phishing defence solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organisation-wide engagement to active email threats. Our collective defence suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organisations in defence, energy, financial services, healthcare and manufacturing sectors that understand how changing user behaviour will improve security, aid incident response and reduce the risk of compromise. To learn more, visit https://cofense.com/.

Contacts for Networks Unlimited

Networks Unlimited, Michelle Naidoo, +27 (0) 11 202 8400,

michelle.naidoo@nu.co.za

icomm, Vivienne Fouché, +27 (0) 82 602 1635, vivienne@pr.co.za

www.icomm-pr.co.za

Media Contact for Cofense™

Nick Lagalante
Global Corporate Communications
COFENSE™
P: +1-571-393-2403
E: media@Cofense™.com