# Phake-Phishing: Phundamental oder Pherrückt?

*Phishing ist der Klassiker unter den Cyberangriffen, denn es ist kostengünstig, effektiv und oft der erste Schritt, um Systeme zu kompromittieren. Kein Wunder, dass Unternehmen ihren Mitarbeitenden mit Simulationen das richtige User-Verhalten bei Phishing-Versuchen antrainieren wollen. Doch helfen diese gefakten Phishing-Tests wirklich?*

Auf dem Papier klingt es einfach: Wer für den Ernstfall übt, ist besser gewappnet. Das gilt im Sport, im Militär, in der Krisenvorsorge – und auch in der Cybersicherheit. Simulierte Cyberangriffe (Red- und Purple-Teaming), Capture-the-Flag Cybersicherheitswettbewerbe oder Planspiele (Tabletop-Übungen) zeigen, dass Vorbereitungen wirksam sind. Warum also nicht auch beim Phishing?

Die Realität ist jedoch komplex. Sophos X-Ops identifizierte vier typische Fallen bei der Umsetzung von Phishing-Trainings: Übungen werden zu reinen Tick-Box-Aktionen, unfaire oder ethisch fragwürdige Simulationen erzeugen Stress, Nutzer werden für „Fehler“ bestraft, und der Fokus liegt oft auf dem Scheitern statt auf dem richtigen Verhalten. Befürworter argumentieren, dass Phishing-Simulationen das Bewusstsein stärken, Instinkte trainieren und eine „Security-First“-Kultur fördern. Kritiker verweisen auf Studien von 2021 und 2025, die nur minimale Effekte auf die Klickrate zeigen – manchmal steigt die Anfälligkeit sogar, etwa durch Ermüdung oder falsche Sicherheit. Schlecht geplante Phishing-Übungen sind nutzlos oder sogar kontraproduktiv. Doch Ignorieren ist keine Option, denn Angreifer setzen weiter auf den einfachsten Zugang: den Menschen.

**Erfolg statt Misserfolg**

„Unbedachte Klicks sind nicht das, worauf der erste Fokus liegt, entscheidend ist, dass ein Reporting folgt“, bringt Sophos-CISO Ross McKerchar das Ziel der Phishing-Tests auf den Punkt. „Wer verdächtige Mails meldet, liefert wertvolle, sofort verwertbare Bedrohungsinformationen. Deshalb gibt es bei Sophos einen gut sichtbaren „Report“-Button, schnelle Rückmeldungen und positive Verstärkung für richtiges Verhalten. Nutzer werden belohnt, nicht bestraft – selbst, wenn sie versehentlich auf einen Link klicken.“

Das ändert die Dynamik: Statt Nutzer als „schwächstes Glied“ zu sehen, werden sie zu aktiven Verteidigern. Mit folgenden Tipps wird die Übung wird zum Lernspiel, nicht zur Falle:

- Die richtige Frequenz finden – weder zu oft noch zu selten.
- Realistische, aber ethisch vertretbare Texte wählen.
- Den Fokus auf positives Verhalten legen, nicht auf Fehler.
- Meldungen und deren Geschwindigkeit priorisieren.
- Blick über den Klick hinaus: Auch Folgeaktionen und Meldungen zählen.
- Alle Teams einbeziehen, um ein realistisches Bild zu erhalten.
- Technische Systeme sollten menschliches Versagen tolerieren.

„Phishing bleibt eine ständige Bedrohung und KI wird Angriffe künftig noch raffinierter machen. Menschen sind dagegen die wertvollste Verteidigungslinie. Richtig gestaltet, durchgeführt und gemessen, stärken regelmäßige Phishing-Simulationen die Wachsamkeit, liefern wichtige Bedrohungsdaten und fördern eine Sicherheitskultur, die echte Angriffe wirksam abwehrt“, so Ross McKerchar.

Wer sich noch näher in das Thema einlesen möchte, kann dies im englischen Blogbeitrag tun.

**Social Media von Sophos für die Presse**
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

**Pressekontakt:**

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de