TitanHQ™

Recent Phishing Attacks and the Fallout for SMBs.

Phishing, now one of the most dangerous security threats businesses face, demands immediate attention. The task of distinguishing a phishing email from a legitimate one has become increasingly challenging as cybercriminals perfect their craft of mimicking trusted senders.

Phishing impacts real people and actual companies. One of the best ways to understand how phishing works is to look at real-life examples to see how phishing attacks affect those at the short end of the phishing rod.

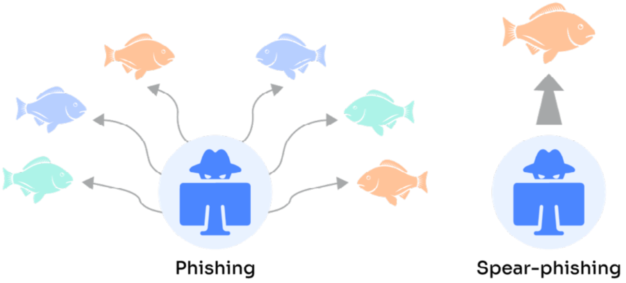
Fresh from our latest report, here are some headline stats about phishing that you need to know for 2024:

- Almost all **(94%)** of firms are victims of a phishing attack. (Source)
- Phishing attackers are becoming more successful at phishing, with **98%** of firms negatively impacted. (Source)
- Phishing attacks are hard to detect and contain, and phishing-related breaches take **295 days** to spot and stop. (Source)
- Spear-phishing, which targets specific roles in an organization, is the most common type of cyber-attack behind scams; conventional phishing is second with **42%** of the attacks. (Source)

Recent Phishing Attacks

Laptop Maker Framework and a Supplier

Spear-phishing attackers targeted an employee at laptop manufacturer Frameworks' supply chain accounting firm (Keating Consulting). Phishers often target supply chain members as this is an easier way to move up the chain and have a lateral impact across multiple customers; Keating Consulting has over **300 customers** who could be impacted by the socially engineered phishing campaign that targeted the organization. During the attack, cybercriminals accessed company records, including outstanding invoice balances. It is believed this was an initial attempt at Business Email Compromise (BEC).



Oktapus and Okta

Okta, a digital identity provider, fell prey to an extensive phishing campaign. Exploiting Okta's IAM reach, the Oktapus group created 169 domains to deceive users. Phishing attacks via SMS, lured employees to Okta-branded sites, stealing **9,931 credentials and 5,441 authentication codes.** Victims included Twilio and Cloudflare.

Norton Fake Antivirus Update

Cybercriminals stole **$34,000** from one victim using fake Norton antivirus renewal subscription phishing emails. The phishing emails displayed a phony invoice for a Norton antivirus update with a phone number to call to cancel the invoice. The email phishing scam became a Vishing (voice phishing) scam where scammers tricked victims into revealing bank details.

Managed Care of North America (MCNA) Dental

Ransomware delivery is primarily achieved using phishing, according to America's cyber-defense agency, CISA. LockBit is a common ransomware variant and is often used to target healthcare. LockBit infected MCNA Dental and saw almost **9 million people** have their data compromised in the attack.

High-Profile Person-Targeted Attacks

In 2022, Trump's re-election campaign account suffered a **$2.3 million** loss due to spear-phishing. High-profile individuals are frequent targets, as seen in the case of Nest Wallet's CEO, Bill Lou. He fell victim to a sophisticated phishing scam, losing approximately **$125,000** through tactics like a deceptive URL and a fraudulent website.

The Guardian

The Guardian is a UK newspaper that became a victim of a ransomware attack initiated by an email phishing attack. The incident compromised the personal data of staff, subscribers, and other readers. The Guardian wrote about the attack, describing it as a **"highly sophisticated cyber-attack involving unauthorized third-party access to parts of our network,"** most likely triggered by a "phishing" attempt."

n promise to battle
st peacetime threat
PM tells Britain: stay i
stop march of coronav
Avoiding the gym? We pick six of the best home workouts
The hellish side of hygiene OCD in the era of Covid-19
The Guardian
Virus 'may last a year and put 8m in NHS hospit
Europe puts

Booking.com

A phishing attack on Booking.com saw the **theft of customer's credit card data.** The phishing emails came from the official noreply@booking.com email address and warned customers that their stay would be canceled unless they supplied bank card details via a linked website. Booking.com believes that the messages involved breaches in the email systems of partner hotels rather than Booking.com's web server.

AiTM and BEC fraud

As per Microsoft, tens of thousands of companies were impacted by Adversary-in-the-middle (AiTM) phishing. This technique involved emails with malicious HTML attachments, often appearing as voicemail notifications. Users prompted to open an attachment ended up on a fake Office 365 login page, leading to stolen credentials. The scam is part of a more significant financial fraud and Business Email Compromise (BEC) strategy executed through phishing-as-a-service (PhaaS) platforms, **targeting over 10,000 companies**

Phishing Protection using PhishTitan

These examples of phishing attacks show that phishing is sophisticated, complex, and often multi-part. This makes for complicated attack scenarios that are challenging to detect and prevent. Modern-day threats are bypassing traditional email security solutions.

PhishTitan is a cloud-based, AI-driven, advanced phishing protection solution for companies using Microsoft 365. PhishTitan natively integrates into M365, augmenting EOP and Defender by catching and remediating sophisticated phishing attacks that Microsoft misses.

PhishTitans' multiple layers of analysis and detection methods offer unbeatable anti-phishing accuracy for zero-day attacks, with minimal false positive results. **Book a personalized demo to see how PhishTitan can protect against the most advanced BEC and phishing threats.**

Book a Demo

TitanHQ™

About TitanHQ

TitanHQ offers a best-in-class SaaS Cybersecurity Platform delivering a layered security solutionto prevent user vulnerability. Our MSP-centric platform enables our partners to generate recurring revenue through the sale of our solutions to SMBs and to scale and effectively manage their businesses.