SecurityAwarenessNews

the security awareness newsletter for security aware people

When Attackers Get Personal

Understanding Advanced Attacks
Thread Hijacking
AI and the Evolving Landscape of Phishing

© 2025 KnowBe4, Inc.

UNDERSTANDING ADVANCED ATTACKS

Annual cybercrime statistics vary from year to year, but one attack method always tops the list: phishing. As a refresher, phishing is a scam in which criminals attempt to steal data, spread malicious software (malware), and defraud people of money.

Many of these attacks involve a generic message sent to several people through various communication methods. Spear phishing attacks, however, are much more strategic. Here is a quick overview of advanced phishing concepts:

The attackers are well-researched. They gather detailed information about their targets from social media, websites, and other public sources.

It's a targeted approach. Unlike generic phishing attempts, spear phishing is often personalized and tailored to specific people, job titles, or organizations.

It's often successful. Past research showed that while spear phishing was involved in only .01% of email-based attacks, it accounted for over 65% of successful compromises.

Many spear phishing attempts use impersonation. To establish trust, it's common for attackers to pose as trusted individuals or organizations known to the target.

These attacks often feature email spoofing. Spoofing is a form of forgery that manipulates email addresses so they appear to come from someone you know.

Spear phishing can lead to major consequences. A successful attack may result in data theft, financial losses, and reputational damages.

These advanced attacks highlight the importance of security awareness for every member of an organization. While spear phishing typically targets high-profile individuals, such as executives, anyone could encounter a sophisticated attack.

So, regardless of your job title, remember you are the last line of defense. Your commitment to security keeps people and organizations safe. Part of that commitment includes always following policy, staying alert, and reporting anything suspicious immediately.

© 2025 KnowBe4, Inc.

THREAD HIJACKING

Thread hijacking is an attack using a compromised email account to steal data or, more commonly, large sums of money. As a simplified illustration, this is the typical flow of how cybercriminals hijack an email thread:

First, the attacker gains access to someone's email account. This is usually accomplished when that person falls for a phishing attack or uses weak passwords. Once inside, the attacker will patiently monitor communications. They are often looking for situations that involve financial transactions. Their goal is to intercept the conversation at the right moment.

For example, as soon as it's clear that funds are ready to be wired, the attacker will send a message using the compromised email account with updated (and fraudulent) wire instructions. Since the message comes from a trusted source in an ongoing communication, the target usually has no reason to think it's suspicious.

Thread hijacking is one example of how important it is to ensure cybercriminals never access your email account. Here are a few ways to prevent that from happening:

Know the Warning Signs

Phishing attacks are the most common way accounts get hacked. Stay aware of typical warning signs, such as threatening language, urgent requests, and unexpected links or attachments. Thoroughly review messages for anything suspicious or odd.

Use Strong, Unique Passwords

A strong password is long, hard to guess, and adheres to organizational policies. Never use the same password twice. Doing so could allow an attacker access to multiple accounts should a password be leaked or stolen.

Enable Multi-factor Authentication (MFA)

MFA is a security feature that requires at least two forms of authentication before access is granted. The key benefit of MFA is that even if attackers steal a password, they're less likely to have access to additional authentication factors.

© 2025 KnowBe4, Inc.

AI AND THE EVOLVING LANDSCAPE OF PHISHING

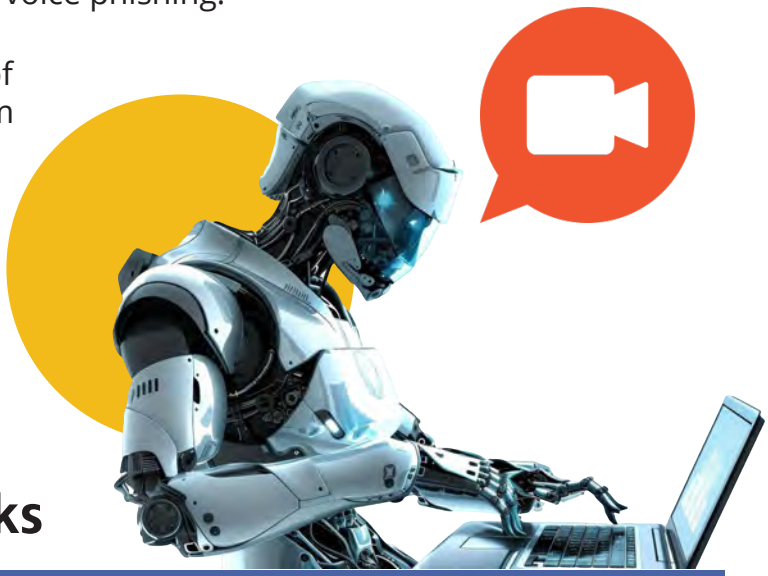
Put yourself into the following scenario:

You work in the finance department and receive an urgent video call invitation with a few of your colleagues and a high-level executive. After a long discussion, you're asked to wire a large sum of money to five separate bank accounts.

Now, imagine learning a few days later that you were the only real person on that call. The other members were generated with deepfake technology — advanced computer algorithms that can maliciously alter video, photos, and audio.

Here's the crazy part: This scenario isn't just a hypothetical. It's based on a real attack that defrauded an organization out of a staggering amount of money. To learn more about it, search these keywords: Hong Kong employee voice phishing.

This advanced attack showcases the powers of deepfakes and artificial intelligence (AI), a form of computer science that simulates human intelligence. AI-powered attacks are expected to evolve and become more dangerous as technology improves.



Beating AI-Powered Attacks

Practice Heightened Awareness

The power of AI cyberattacks means that everyone needs to take extra precautions as a part of their daily routines. This is especially important when handling requests for money or confidential information. Thoroughly review these communications to identify anything that seems off or asks you to do something you normally wouldn't.

Utilize Zero Trust

Zero trust is a security model that assumes everything is untrustworthy until proven otherwise. The main concept is "never trust, always verify," which is a great approach to all things security. Never assume someone is who they claim to be.

Don't Underestimate Your Value

While it might seem unlikely that you'll encounter advanced attacks, it's important to remain prepared for them. Even if you're not in a position to transfer money, attackers view every member of an organization as an opportunity to gain unauthorized access.

© 2025 KnowBe4, Inc.