Four Emerging Phishing Techniques and How to Detect Them

Introduction

Phishing isn't just an entry point for cybercriminals—it's the most effective way to breach organizations, steal credentials, and deploy ransomware. Attackers are weaponizing AI, social engineering, and deepfake technology to make phishing nearly indistinguishable from legitimate communication. If your defenses aren't evolving, you're already compromised.

Industry reports highlight the growing risk:

- 2024 Ponemon State of AI in Cybersecurity Report: 83% of organizations experienced a phishing-related security incident in the past year.
- Gartner Top Trends in Cybersecurity for 2024: Over 90% of cyberattacks start with phishing, often leading to compromised credentials and lateral movement.
- Forrester's Top Cybersecurity Threats in 2024: 78% of organizations experienced multiple breaches in the past year, with a significant portion originating from sophisticated phishing campaigns.

As phishing techniques grow more advanced, security teams must adopt a proactive approach to detection and response. This paper breaks down four emerging phishing tactics and dellivers actionable strategies to identify and mitigate them.

The Four Emerging Phishing Techniques

Cybercriminals continuously evolve their tactics to bypass security measures. Below are four emerging phishing techniques that pose serious threats to organizations:

1. Impersonation and Credibility Manipulation

Attackers exploit trust by impersonating executives, business partners, or vendors using lookalike domains, fake display names, and compromised accounts. They leverage:

- Homoglyph domains (for example, "mìcrosoft.com" instead of "microsoft.com")
- Fake SSL certificates to add legitimacy
- Social engineering tactics to create a sense of urgency

2. AI-Powered Phishing Campaigns

Cybercriminals use AI-driven tools to generate hyper-personalized phishing emails, deepfake voice messages, and realistic fake websites. Their methods include:

- AI-generated phishing emails that mimic internal corporate communication
- Deepfake voice and video impersonation of executives
- AI-powered bots that engage in real-time phishing conversations

3. Credential Theft via Spoofed Login Pages

Instead of using malware, attackers trick victims into entering credentials on fraudulent login pages hosted on legitimate services like Google Firebase. Attackers:

- Create highly realistic login portals to steal usernames and passwords
- Use deceptive redirects to avoid security detection
- Exploit commonly used services to bypass domain reputation checks

4. Business Email Compromise (BEC) and Financial Fraud

BEC scams manipulate employees into taking unauthorized financial actions by posing as trusted figures within an organization. Common tactics include:

- CEO fraud, where attackers impersonate executives requesting urgent payments
- Invoice fraud, tricking finance teams into paying fake invoices
- Gift card scams, where attackers pose as leadership demanding gift card purchases

Strengthening Your Organization's Phishing Detection Strategy

Phishing detection isn't just about technology—users play a critical role. But relying solely on employees to spot phishing attacks is a flawed strategy.

How Attackers Exploit Trust:

- **Sender manipulation**: Attackers frequently use lookalike domains to deceive recipients. To counteract this, security teams must implement domain verification, scrutinize SSL certificates, and use automated tools to detect spoofed sender addresses in real time.
- **Malicious links**: Users may hover over a link, but attackers often disguise final URLs through multiple redirects. Security teams should analyze link resolution paths and SSL details.
- **Weaponized attachments**: An unexpected, password-protected Word document should be considered highly suspicious.

EXABEAM INSIGHTS

Legitimacy Should be Found in Every Detail

→ **Attackers exploit trusted file hosting services like Dropbox and Google Drive to deliver malicious content. Exabeam behavior analytics detect abnormal domain registrations and network traffic patterns, exposing hidden phishing operations.**

Multi-Layered Phishing Detection

No single control is enough. Organizations must combine:

- Security awareness training: Educate employees on evolving phishing threats and AI-powered attacks.
- Behavior analytics: Detect anomalies in user activity, authentication patterns, and email interactions.
- Real-time visibility: Monitor email, endpoint, and network activity to identify phishing attempts before the damage occurs.
- Threat intelligence: Integrate feeds to proactively block phishing indicators before they reach users.

How Exabeam Helps

Exabeam SIEM and UEBA solutions provide deep visibility into phishing-related threats by:

- Detecting unusual login attempts and multifactor authentication (MFA) fatigue attacks
- Correlating endpoint and network activity to uncover phishing payload execution
- Identifying anomalies in user email behavior and authentication patterns

Phishing isn't going away—but you can stop it before it becomes a breach. Exabeam delivers the visibility, detection, and automation needed to stay ahead of attackers. Request a demo today.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity leader, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at
www.exabeam.com →