The Impact of Phishing

What’s Inside

- Intro
- Phish tales
- Primary Impacts
  - Financial
  - Productivity
  - Investor and consumer confidence
  - APT
- Recommendation
- How Okta can Help

Introduction

You're probably familiar with phishing at this point.

You know, those emails that pretend to be from your bank, social network, or email provider and try to steal your credentials. It's an old, established, and (sadly) effective tactic.

If you've been unfortunate enough to fall victim to this type of attack, you are not alone, and don't beat yourself up over it.

Phishing is a lucrative game. And, like any criminal enterprise, its participants continually refine their tactics to be more effective and target even more valuable marks.

Phishing has been with us since the internet first started entering people's homes. The first incarnation emerged in 1996, when criminals sought to steal the login credentials of AOL users by impersonating employees of the early internet pioneer.

Phish Tales

Perhaps you have heard a multitude of tall tales about phishing attacks. We're here to tell you that this isn't something that only old people and young children fall for in their personal digital journeys.

This is a viable threat to organizations of any geo-location and size. Successful phishing scams can have a devastating impact. Even phishing attacks that target an organization or company affect the individuals who work for that organization, or customers and partners of that organization.

It's estimated over one in five data breaches involve phishing. There are several types of phishing attacks, including standard, spear, clone, SMS, voice and whaling. Some target an entire company, while others prey on senior staff.

In this ebook, we will take a closer look at the financial, productivity, Advanced Persistent Threats, and reputational impacts that businesses experience as a result of success phishing attacks.

Phishing scams are the fraudulent attempt to gain possession of sensitive data or information such as passwords, usernames, personal identifying information, trade secrets, and more. Cyber attackers typically use email campaigns, bogus websites, instant messaging, and text messaging to fool individuals within a company to disclose this information, download malware or ransomware, or both.

No matter how it's delivered, a phishing attack poses a substantial risk to your company, regardless of its size or industry.

A successful attack can result in the following possible outcomes:

Tangible:

- Financial exposure and extortion
- Data exfiltration such as PII and IP
- Disruption of operations
- Account takeover
- APT – Malware and ransomware

Intangible:

- Reputational damages
- Public scrutiny – Security practices come under question
- Customer churn
- Attack campaigns
- Lost partnerships and contracts

Financial

Nearly every company that falls victim to a phishing scam faces financial consequences. Along with the direct costs of the breach, phishing attacks on company personnel can also result in fines from various regulatory bodies for rule violations. The damages from stolen customer data can be steep, and other penalties can be astronomical.

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over three years.

This includes the costs of fending off an attack, recovering from an attack, experiencing depreciating stock value, and incurring regulatory fines associated with the incident if regulators discover that your business didn't implement the proper security mechanisms.

You will need extra funds to manage Identity protection: and compensation of customers or employees whose data was stolen following a phishing attack.

An attacker could also transfer funds from a company's account through impersonation via phishing.

Violating regulatory requirements such as HIPAA, PCI, and European GDPR may attract heavy fines. The extent of the fines depends on the industry and the scope of the breach.

In 2019, the Federal Trade Commission (FTC) ordered Equifax to pay up to $700 million over their 2017 data breach, which exposed the personal information of nearly 150 million Americans. It was one of the biggest data breaches in history, and the FTC wasn't messing around.

Productivity

Data breaches or system compromises arising from phishing attacks cause business disruption.

Following a successful phishing attack, a business will spend a great deal of time trying to recover lost data and investigating the breach with little left for actual business. Employees productivity will also take a hit as many systems are put offline for reconfiguration and cleaning.

But in cases with a material outcome — like a loss of money or data — 41% of organizations take a day or more to recover.

Other productivity losses can come in the aftermath of a virus or malware infection due to a successful phishing attack, as everyone is redirected to putting out the immediate security fire.

On average, U.S. businesses stand to lose $1,819,923in productivity because of phishing scams.

APT

An advanced persistent threat (APT) isa broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a networking order to mine highly sensitive data.

The consequences of such intrusions are vast and include:

- Intellectual property theft (e.g., trade secrets or patents)
- Compromised sensitive information (e.g., employee and user private data)
- Sabotage of critical organizational infrastructures (e.g., database deletion)
- Total site takeovers

Once an attacker’s found their way into your network, they can install malware or ransomware, which could cause system outages and other nasty disruptions.

Ransomware is one of the costliest forms of malware, and it’s often delivered through a phishing email. As soon as the ransomware infects one device, it seeks out others on the network to infect, taking down an entire office.

Ransomware encrypts files, making them unusable. The hacker demands a ransom, usually in bitcoin, in exchange for a decryption key.

APT attacks differ from traditional web application threats, in that:

- They’re significantly more complex.
- They’re not hit and run attacks — once a network is infiltrated, the perpetrator remains in order to attain as much information as possible.
- They’re manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets.
- They often aim to infiltrate an entire network, as opposed to one specific part.

Reputational

Reputational damage fuels the fire, sometimes with astronomical costs.

When investors and consumers lose confidence in a brand, they tend to shy away from supporting the company. They purchase fewer items or take their business elsewhere.

Investors have a moral dutyto ensure cybersecurity initiatives are given priority during all stages of business development.

Once information about an attack appears on news and social media outlets, the brand's image is immediately hurt.

Think about a restaurant – when there's a claim about food poisoning or a health concern, you're less likely to go there. It's a similar mentality.

Consumers begin to worry that it's unsafe to do business with the organization. This fear leads to lost confidence, which can cause consumers to drop the damaged brand for a competitor.

Customers can file lawsuits, or organizations face fines for non-compliance with data protection regulations.

When a breach compromised Facebook's user data in 2018, the company's total value dropped by $36 billion, a loss it's still recovering from.

One of the most prominent breaches in history happened in 2013, when hackers stole credit and debit card numbers from 40 million Target shoppers and personal contact information from another 70 million.

Target met a swift fallout, spending 10s of millions of dollars on legal fees, customer reimbursements, software updates, and more. They faced over 140 lawsuits and saw profits plummet by nearly 50%. due to eroded customer trust.

Recommendation

Due to the psychological and sociological aspects of phishing,even highly knowledgeable individuals may fall prey.(Admit it: You've accidentally clicked on something you shouldn't have.) Bluntly – it's unfair to always blame the user for falling for these attacks.

An Identity-first approach to security integrates with your entire security stack and empowers users to be the strongest line of defense.

Now, more than ever, organizations need security tools that prevent phishing attacks and integrate easily with their existing ecosystems without disrupting productivity.

Phishing-resistant authenticators are a critical tool in personal and enterprise security that should be embraced and adopted. They are not, however, a silver bullet. Ideally, they need to be paired with a comprehensive Identity-powered security approach integrated with a broader security ecosystem that includes:

- *Centralized Identity management*
- *Phishing-resistant authenticators*
- *Adaptive access policies*
- *ITDR (Identity threat protection)*
- *PAM (Privileged access management)*
- *Automated workflows for remediation*
- *End-user notifications*

How we can help

Okta offers a strong,identity-first approach to security which incorporates phishing-resistant passwordless authentication with secure sign-in policies and contextual access controls based on Zero Trust principles to prevent your organization from phishing attacks. Go beyond MFA and SSO to prevent phishing from impacting your organization.

We do this by providing products and features that:

Prevent

- Implement preventive security measures with HealthInsights
- Limit the attack surface with ThreatInsights
- Enhance controls for WebAuthn + passkeys management
- Enforce adaptive access policies
- Enable secure, phishing-resistant access — throughout the enterprise

Detect

- Enforce security checks for unmanaged devices
- Intelligent Identity Threat Detection alerts on malicious activities
- Detailed analysis with enhanced logging for faster detection

Respond

- Improved response times with automated workflows
- Take action with Universal Logout to isolate user activities
- Enable self-service actions for remediation

Turn users from the ‘weakest link’ in your security ecosystem into your strongest assets with Okta.