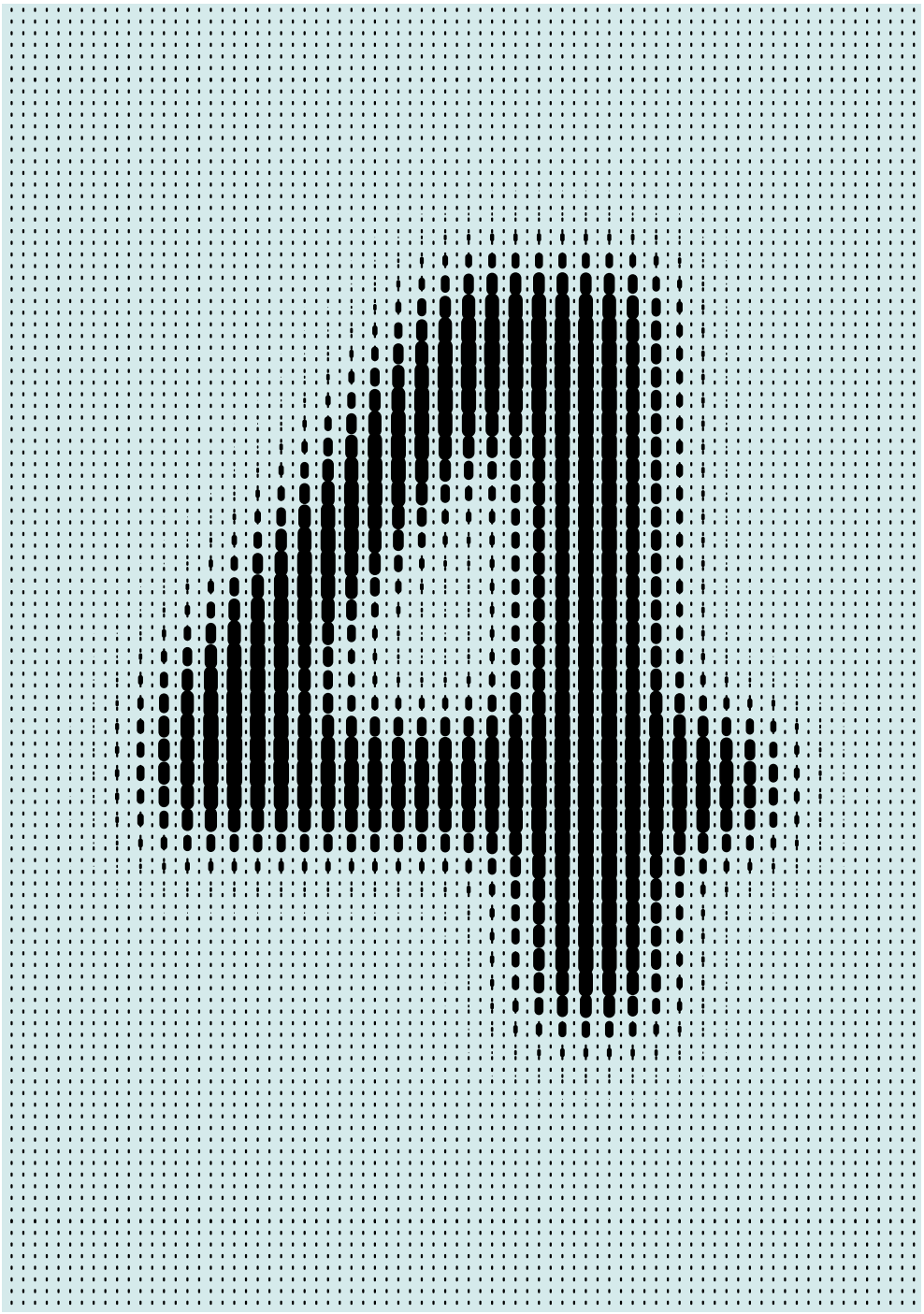
Whitepaper

November 2020

Four Myths About Credential Phishing You Can't Ignore

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Contents

Introduction

While ransomware, securing the cloud, and a sprawling Internet of Things are keeping our CISO's up at night—a consistent threat is plaguing their employees. Credential phishing. Zero-day vulnerabilities are overrated, says noted security guru Bruce Schneier; credential stealing is how attackers are getting into our networks.[1] And the stats agree with him. The 2017 Verizon Data Breach Investigations Report cites 81% of attacks involved stolen credentials.[2] Understanding phishing means understanding one of the most common methods used by attackers to successfully breach and maneuver within our networks, and to do that we need to dispel a few myths.

Credential phishing is the practice of stealing user ID/email address and password combinations by masquerading as a reputable or known entity or person in email, instant message, or another communication channel. Attackers then use the victim's credentials to carry out attacks on a secondary target.

Common Misconceptions

When it comes to phishing, knowledge is power. We tend to underestimate the impact of phishing on the enterprise and assume our existing defense strategies are sufficient to combat these attacks. We've identified four key misconceptions about credential phishing:

[1] Bruce Schneier. "**Credential Stealing as an Attack Vector.**" Schneier on Security. May 04, 2016.

[2] "**2017 Data Breach Investigations Report (DBIR).**" Verizon. 2017.

Myth 1: Enterprises Are Not the Target, Consumers Are

To start with, most of us thought phishing was a consumer-based threat. Yes, most phishing is still aimed at gaining access to an individual's bank account. Yet financially motivated attackers are also seeing huge value in targeting organizations, for example, stealing patient records to commit insurance fraud, stealing IP and selling it on the black market, or hacking into POS systems. The Verizon DBIR reported that 73% of breaches were financially motivated–many of them carried out by nation-state affiliated actors.[3]

Consumer phishing has evolved into an enterprise attack because:

1. Employees reuse passwords from their personal accounts on their business account

2. Attackers have learned that they can get inside our networks by exploiting our employee's personal accounts

The average user has over 40 services registered to one email address, yet only five unique passwords, according to Experian.[4] Those just might be the same passwords used on an employee's work account.

What's more, our employees are leveraging corporate connectivity; they're reading and responding to personal email and clicking phishing links while connected to the corporate network. Enterprises are seeing phishing at all hours, though the volume of clicks that lead back to malicious URLs is significantly higher on weekdays.

Monday	18%
Tuesday	21%
Wednesday	21%
Thursday	22%
Friday	16%
Saturday and Sunday	1%

According to Wombat State of the Phish report, click through to malicious phishing sites is highest on Thursday.[5]

[3] "**2017 Data Breach Investigations Report (DBIR)**". Verizon. 2017.
[4] Mike Delgado. **"Experian Reveals the Five Key Factors That Make People & Business More Vulnerable to Cyber Fraud"**. Experian. May 19, 2016
[5] "**State of the Phish 2017**". Wombat Security Technologies. 2017

Myth 2: Phishing Is All About Opening Attachments

Okay, you say—but the danger in the phish is the attachment, right? Not necessarily. As of late 2016, researchers saw more phishing lures lead victims to URL-based threats that originate from multiple channels including SMS messaging. Here's how it works:

1. The first step is for the attackers to compromise a legitimate website or register a fake domain. In late 2015, phishingwent commercial. Today's attackers buy Phish Kits containing all the necessary attack components. As an alternative, Phishing-as-a-Service can be employed.

2. Once the environment is established and the targets are identified, phishing messages are sent to the victim who is often compelled to investigate the message claim. Some of the most effective messages targeting both consumers and employees refer to online order delivery or business financial transactions.Once the victim clicks the link, they are sent to a spoofed site that requests personal information. One of two things happen next:

    - The victim enters their current user ID and password into the spoofed site, and that data is forwarded onto the attacker, or
    - The spoofed site contains malware that is automatically downloaded onto the victim's device to gather all of the user's credentials stored on the device or in browser memory

3. The victim's data is sent to a drop email account or forwarded to another domain controlled by the attacker.

4. Once attackers acquire a victim's credentials they can carry out the next phase of their attack which is to either:

    - Enter the credentials into as many websites as possible using automated scripts, often called credential stuffing, or
    - Enter the stolen credentials directly into corporate resources gaining unfettered access to your network and data

The likelihood of these attacks occurring is rising, and according to a recent report from Akamai, "more than 40% of global log-in attempts are malicious thanks to bot-driven credential stuffing attacks".[6] Enterprise users are targeted using similar tactics with one added ingredient: social engineering. Today's attackers are organized and often state-sponsored or at least well-funded. They do their research and target key employees—typically those who handle financial transactions or executives—and invent a believable story.

[6] "**Fourth Quarter, 2017 State of the Internet / Security Report**". Akamai. 2017.

Myth 3: My Employees Can Be Trained Not to Click

Year-over-year data shows that employees are becoming savvier, and are less likely to fall prey to phishing attacks. This indicates that more companies are investing in phishing awareness, and that simulated phishing does make a difference. Training your employees to avoid clicking links and to report suspicious email can reduce the mean-time-to-detection from days to hours,[7] according to PhishMe, a leader in phishing simulation and awareness training.

However, training may not address the most difficult phishing lures for employees to avoid—those with a valid business context.

Business Email Compromise (BEC) is highly personalized for your employees, and the attacker's aim is to trick your employee into conducting valuable financial transactions. Using stolen credentials, an attacker can compromise the internal email accounts of key executives to access sensitive corporate data. While many organizations are training their employees to detect phishing, Symantec reported seeing approximately 8,000 business targets a month with BEC.[8]

[7] "**Enterprise Phishing Susceptibility and Resiliency Report**". PhishMe. 2016
[8] "**Internet Security Threat Report: Email Trends Report 2017**". Symantec. 2017.

Myth 4: Security Controls at My Perimeter Are All I Need

Previously, detection and blocking were effective components of a layered defense against phishing. When sensitive corporate resources were exclusively behind the firewall, organizations had more centralized control of what came through the traditional perimeter. With the move to cloud apps, traditional perimeter controls often can't be applied in the same way. Moreover, the ease and speed at which malicious domains can be deployed to support targeted phishing attacks renders our traditional perimeter defenses only partially effective, as blocking domains becomes a never-ending game of whack-a-mole that leads to false positives and false negatives.

You can establish upstream controls such as a Domain-based Message Authentication, Reporting & Conformance (DMARC) policies. These policies make it difficult for attackers to successfully phish. They allow only messages with both valid Sender Policy Framework and DomainKeys Identified Mail, and if implemented properly DMARC can prevent spoofing of the header address.

Email controls are one thing—but what about SMiShing? Attackers are finding new ways to deliver phish that entirely avoid the email gateway, such as SMS and social media. You can, and should, counter with security on all of your endpoints including mobile, but perimeter controls will not directly address the problem of credential phishing. It's access to your network and your data that attackers are after and you can prevent their entry by taking passwords off the table altogether.

The Best Defense Includes Identity-Driven Security

It's clearly time to rethink our defenses against phishing. We know that the enterprise is a target for phishing—both directly and indirectly. We know that our employees often reuse passwords and that they can easily be tricked into handing over this information.

Successful phishing prevention starts with placing identity at the center of our security strategy.

Centralize identity managements

Identity represents a critical control point that, once addressed, dramatically improves security across the enterprise. We can protect users, and thus our organizations, from theft and account takeover by centralizing Identity and Access Management (IAM). To do so, we simply need to ensure strong authentication across all services, everywhere. You can establish Single Sign-On to the entire enterprise using the Okta Identity Cloud. Workday, Microsoft Office 365, Salesforce, etc.—Okta integrates seamlessly with the applications you are already using. We integrate with over 5,000 cloud applications, as well as your legacy IT infrastructure and devices.

Stop playing whack-a-mole

Instead of attempting to detect and block all domains associated with phishing, you can implement a comprehensive security layer using intelligent, context-driven authentication found in Adaptive Multi-Factor Authentication (Adaptive MFA). Adaptive MFA uses a diverse set of second factors to authenticate a login attempt, such as third-party hardware tokens, SMS one-time use codes, acknowledgment through a mobile app, biometrics, and unique PINs.

Adaptive MFA adjusts to the access behaviors of the user to determine when to deny access or when to "step up" access and request additional verification. This technology addresses the entire digital profile including the user, device, and network. Is the user attempting to connect from an unknown device? Are they on a trusted network or out-of-band? With this information, your team can dynamically adapt security and authentication policies to enforce step-up authentication for each user and situation.

Adaptive MFA is especially effective because it doesn't come at the expense of the user experience. Flexible policies can prompt for MFA only in certain situations to minimize disruption, such as when users are accessing the resource for the first time or when the user is off the corporate network.

Limit accounts and your attack surface

Reduce your attack surface and automate lifecycle management. Better management equals improved security. You can eliminate blind spots by knowing who has access to what; however, account management can be too time consuming for IT to easily maintain. Okta is centrally managed and automated which helps to ensure accurate entitlements and allowing you to scale provisioning, deprovisioning across all users, groups, and permissions policies. Onboarding becomes turnkey. Admins have at-a-glance visibility into users access to every app, service and data store.

Improve your response time

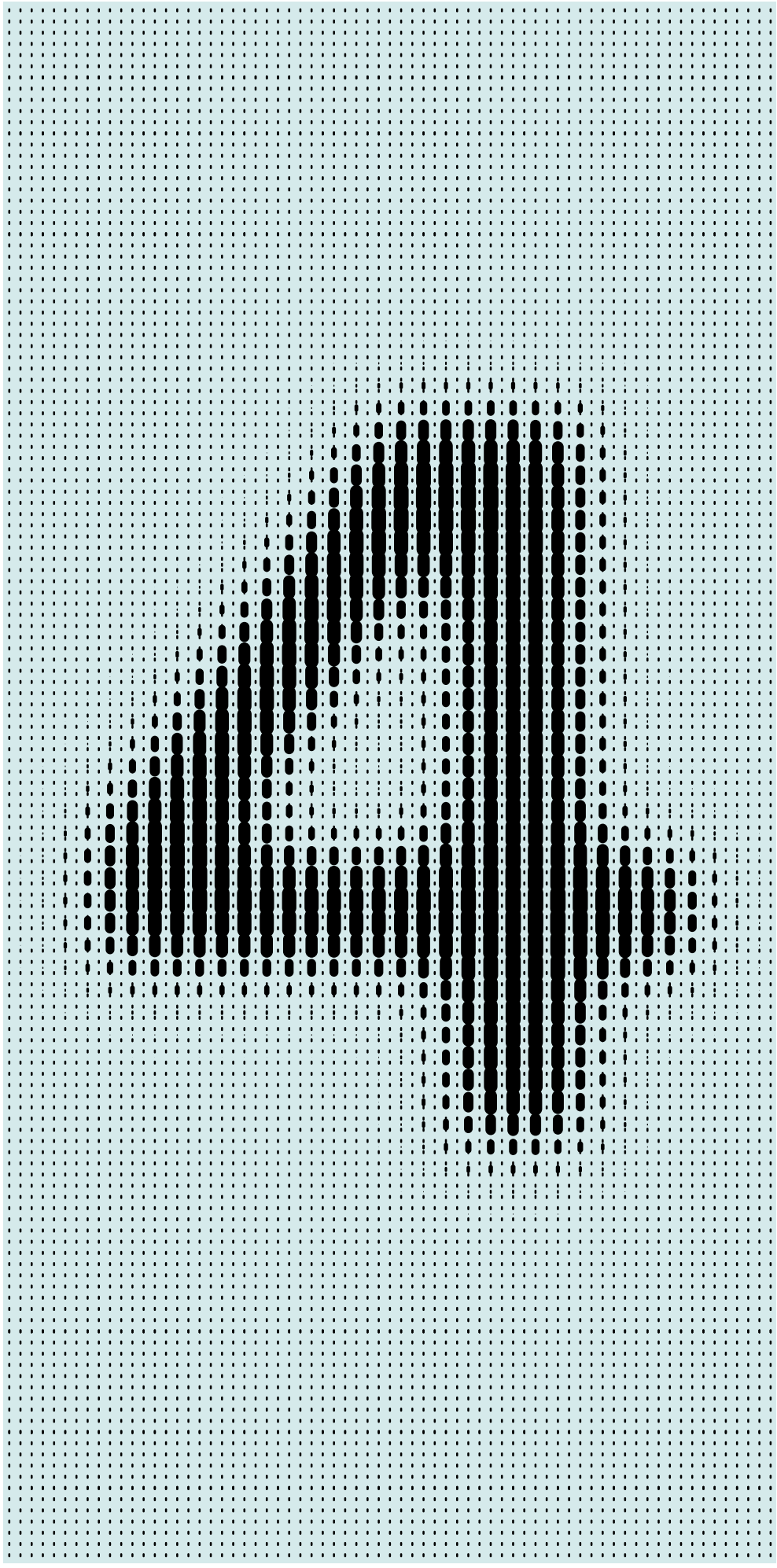
Last but not least, add real-time visibility into authentication events. Connect your IAM directly to your security infrastructure and help your security teams to reduce containment and mitigation time. With Okta real-time authentication, data is accessible by one syslog API. Identity events are seamlessly tied to security management tools like Splunk, ArcSight, and IBM QRadar, among others. You can take immediate action to challenge account takeover attacks as they occur individually or in multiples across your enterprise. You need identity events to be seamlessly tied to security management tools so that you can enrich correlation and ultimately improve response time.

The Truth About Credential Phishing Is That It's a People Problem

Regardless of how well you train your employees, sophisticated social engineering tactics will have a non-trivial success rate. To mitigate this risk, security-conscious organizations are increasingly putting identity and access management at the center of their security strategy. As a first step, place Adaptive MFA and Single Sign-On (SSO) in front of business critical applications—cloud, mobile, and on premise. Not only will you strengthen your authentication, but you will also be improving the employee experience by eliminating password management across apps. You can phase these changes into your enterprise with smart policies that only ask for step-up authentication in the riskiest situations or for your most privileged users. Offering the flexibility and assurance of centralized identity management with SSO and MFA, IT will enjoy the ease of administration and fewer tickets.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.



okta