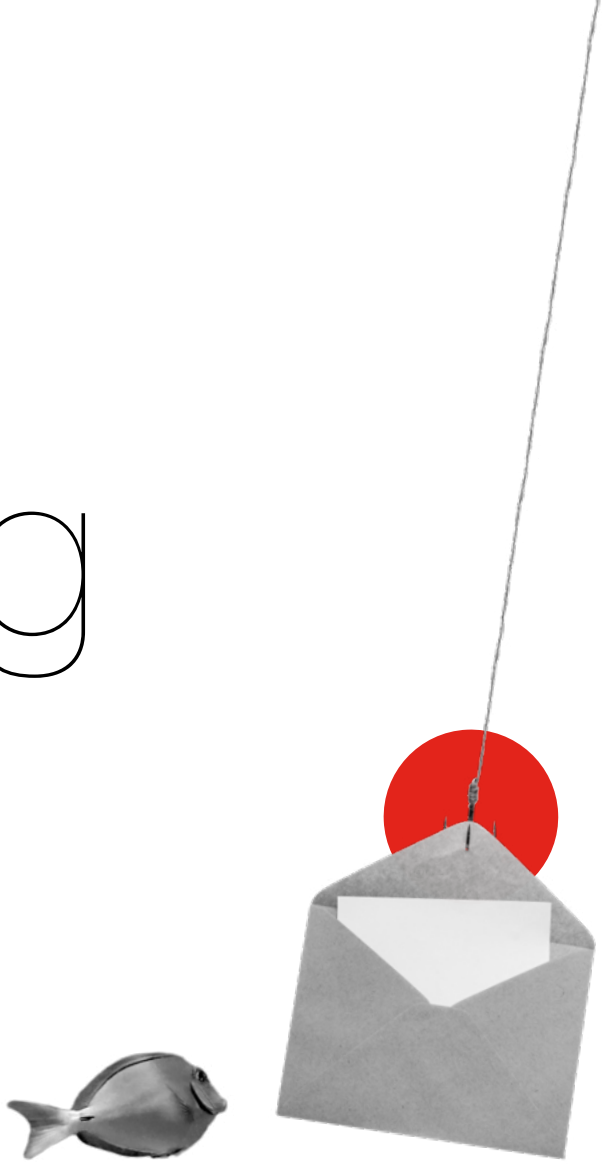
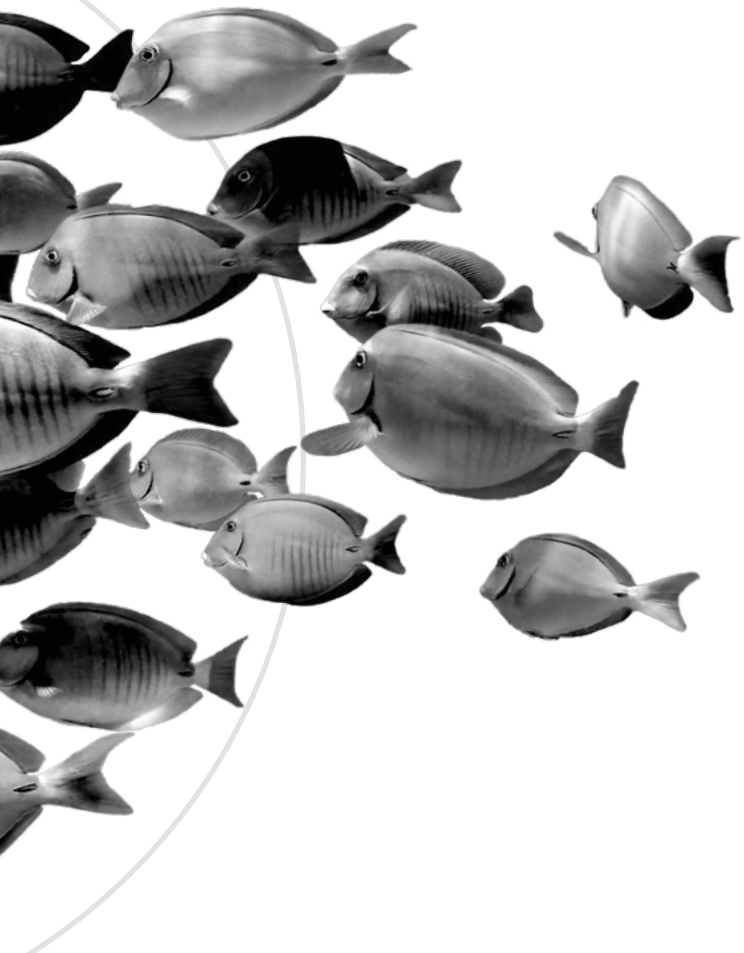
ANATOMY OF A MODERN

Phishing Attack





“

Phishing is an insidious problem where attackers prey on human nature. These attacks are an attempt to gain access to systems and data that they would not otherwise be privy to at all. By relying on socially engineering their victims by using methods such as dark patterns, the attackers utilize stolen credentials for financial gain in many cases. Security controls to limit the access of an attacker are essential to shore up enterprise defenses.

Multi-factor authentication (MFA) is a key tool that enterprises can use to mitigate the phishers’ attempts to utilize passwords that they may collect in the course of a breach. The ability to verify devices and apply adaptive policies will limit attackers’ pivot options. The final column supporting this approach is the implementation of user behavior analytics (UEBA) which provides for greater situational awareness for the enterprise defenders when warding off phishing attacks.”

Dave Lewis

Advisory CISO, Duo Security

ANATOMY OF A MODERN

Phishing Attack

CONTENTS

Increasing Sophistication of Phishing Attacks

IT security teams today face the daunting task of defending an extended perimeter and attack surface due to the increased use of cloud services and the sheer volume of mobile devices that access corporate applications. Enterprise use of cloud apps continues to climb, while employees typically use multiple devices for work to access the many cloud services.

The recent shift to remote work has further blurred the line between personal devices and corporate-managed devices as employees use them interchangeably for work and recreation. While organizations were forced to adapt to a distributed workforce at an accelerated pace, the dependency on traditional technologies and the quick deployment of new technologies have created security **gaps**[1] around connecting devices and trusted access.

According to Verizon's ***2020 Data Breach Investigations Report (DBIR)***[2], 67% of breaches were due to credential theft, errors and social attacks. This statistic indicates that hackers are focusing their efforts on social engineering and spear-phishing tactics to gain trust of unsuspecting victims and compromise their credentials. Sophisticated attacks are becoming increasingly common as hacking and phishing tools, along with documentation on how to use them, are readily available online to hackers. This has significantly lowered the barrier for entry for hackers with time and resources to target organizations, to gather information about security controls that organizations have implemented, and to execute an attack to bypass those controls.

Social Engineering

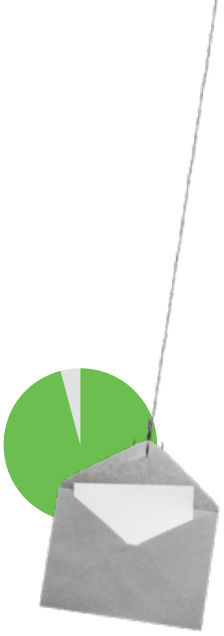
According to the Cybersecurity and Infrastructure Security Agency (CISA), **social engineering**[3] uses human interaction (often through email or phone calls) to obtain or compromise information about an organization or its computer systems.

Social engineering uses psychological manipulation of people in order to get them to perform a specific action or divulge confidential information. Through information gathered by research and manipulative interactions, social engineers may be able to piece together enough information to infiltrate an organization's network and impersonate an actual employee. The hacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and may even offer credentials to support that identity.

Spear Phishing

Spear phishing or targeted phishing is a form of social engineering tailor-made for the individual or organization that receives it. Like regular phishing, the goal of this attack is to acquire sensitive information, install malware, or steal credentials. Unlike regular phishing, spear phishing takes advantage of an individual's personal motivations, interests and incentives to encourage them to fall for the attack.

These types of attacks are opportunistic in nature, taking advantage of the human element of an organization's security. Even the most technologically savvy employees can fall victim to a well-designed social engineering attack. And that's exactly the situation that played out in the high-profile breach we discuss in the case study below.



96%

of social engineering attacks are sent via email. (**2020 DBIR**)

30%

of phishing-related breaches occur to small businesses. (**2020 DBIR**)

80%

of phishing websites have SSL encryption enabled. (**Statsia**)

74%

of phishing websites use HTTPS protocol. (**Statsia**)

CASE STUDY:

A Recent High-Profile Targeted Phishing Incident

What Happened?

In 2020, hackers targeted a popular company through social engineering and organized phishing attacks. Within 24 hours, the hackers gained access to the corporate network, compromised credentials that had access to critical internal systems and took over high-value user accounts on the platform.

How Did It Happen?

STEP 1

Social Engineering

Hackers executed a social engineering attack by calling several employees claiming to be from the organization's IT help desk. Like many organizations enabling their employees to work from home, the company depends on a virtual private network (VPN) for remote access. And since switching to remote work, VPN issues were common at the company. The hackers used this pretext to trick victims into logging into a phishing website by pretending they were responding to a reported VPN problem.

STEP 2

Targeted Phishing

When some employees acknowledged the problem, they were directed to a credential phishing website that looked identical to the legitimate corporate website. The hackers had taken efforts to host the fake login page on a similarly named domain. As the employees entered their credentials into the phishing website, the hackers gained access to those credentials and simultaneously entered the information into the legitimate VPN login page. The hacker's login generated an MFA request and some of the employees authenticated themselves assuming that the request was generated from their login (to the fake website). This allowed the hackers entry into the corporate network.

STEP 3

Lateral Movement

The initial account that was compromised did not have access to the critical internal tools that the hackers wanted to infiltrate. But once inside the network, the hackers could navigate to various information systems and learn more about the internal processes.

They were able to view internal websites that contained information about accessing critical internal applications and systems which the employees had access to. Armed with this information, the hackers then targeted employees who had the access they wanted by using the same social engineering and phishing tactics. The hackers succeeded in compromising the employee credentials to gain access to critical internal systems — and ultimately took over high-value user accounts on the platform.

Authentication Best Practices

to Prevent Sophisticated Phishing Attacks

As the above case study reveals, compromised credentials and access to the right account allows hackers to infiltrate an organization's internal system, in spite of using devices that are not known to or inventoried by the IT teams. To prevent such sophisticated attacks, organizations must consider implementing strong authentication and authorization controls that verify users' identities and their devices' trustworthiness.

Here are some best practices that can help organizations prevent sophisticated attacks by adopting an identity-centric approach to security:

1.

Implement Multi-Factor Authentication (MFA)

Passwords are low hanging fruit for hackers; they are hard for users to remember and for IT to secure. Requiring MFA is a critical security control that can reduce the risk of unauthorized access when passwords are stolen or compromised. There are several user authentication methods available for MFA – but not all MFA methods are equal. Using SMS or text messages as the authentication method for MFA is vulnerable to compromise as the one-time codes can be easily intercepted or phished using readily available online resources such as **SS7 intercept services**[4] or **Modlishka**[5].

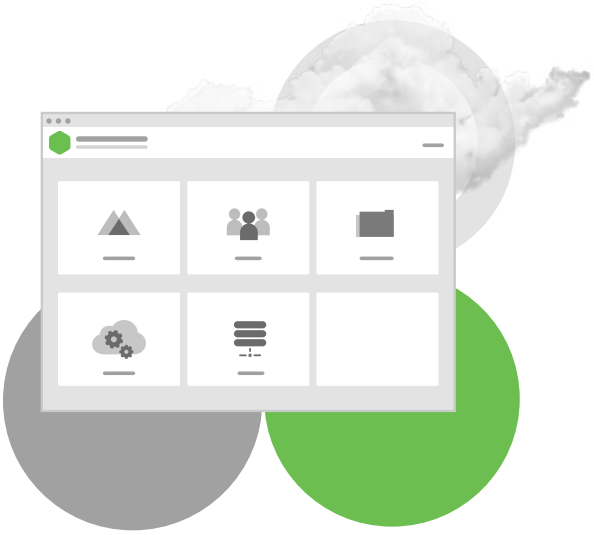
Mobile "push" notification is a more secure authentication method for MFA because it can not be intercepted by hackers. Wherever possible, use **FIDO-based**[6] (Fast IDentity Online, an open industry standard for strong authentication) **security keys**[7] that leverage WebAuthn and provide the highest level of assurance for authentication because it can not be intercepted or phished.

Bonus: Protect Your MFA Implementation

Typically, MFA solutions use secret keys (credentials) to integrate with applications to enforce the additional authentication factor. If these secret keys are not safeguarded, hackers can steal them and compromise the MFA implementation. The secret keys should be treated like passwords and must be securely handled and stored in order to maintain the security and integrity of the critical access control that is MFA. It is recommended to rotate the secret keys in case of a suspected compromise.

2.

Reduce Reliance on Passwords With Single Sign-On (SSO)

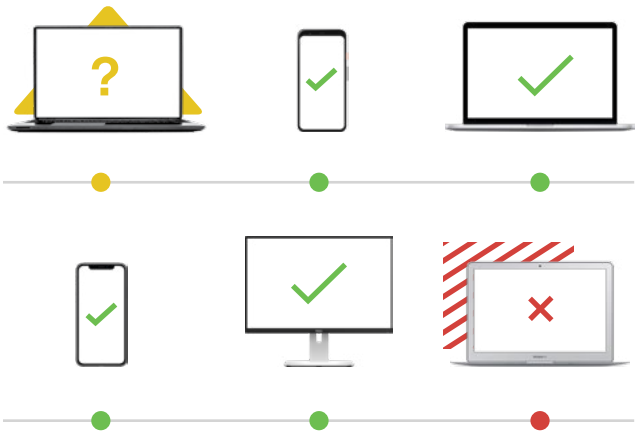


An average enterprise uses **over 1,000 cloud apps**[9] today, and employees typically need to access **more than 10 apps**[10] to perform their daily tasks. That's too many passwords for humans to keep track of and results in password fatigue. In the future, providing a passwordless authentication option wherever possible will mitigate many password-related problems, but for now, implementing single sign-on (SSO) along with MFA is a great way to start the passwordless journey without compromising on security.

For end users, SSO provides access to multiple applications with a single login (using one set combo of username and password). Reducing the number of passwords a user has to remember and the times one has to enter them eliminates bad password habits such as password reuse. For administrators, SSO serves as a unified point of visibility for authentication and access logs, and an effective policy enforcement point in the authentication workflow to enforce security policies for each application depending on its risk profile.

3.

Maintain a Detailed Device Inventory



Many organizations are embracing varying levels of bring your own device (BYOD), and this trend has been exacerbated by the recent boom in remote work. BYOD enables employees to use multiple devices, including personal devices, for work. Multiple devices means multiple operating systems and their versions. The right tool should help IT teams to maintain an up-to-date inventory of all devices and the associated users.

4.

Verify Device Trust as Part of the Authentication Workflow

The authentication workflow must take into consideration the security status of the device used and grant access only if it meets the requirements set by the organization. Major operating systems regularly issue critical security patches that need to be installed. Verifying that updates are installed prior to granting access adds another layer of security.

For critical internal systems, access must be granted only to company managed devices. For hackers, this raises the bar that they need to clear in order to successfully gain access to internal systems. Organizations can significantly reduce the risk of a targeted phishing attack by limiting access to internal systems only from managed devices and preventing access from risky or unknown devices, even when the user's credentials are used, combating compromised credentials.

> "There are primarily three ways you can authenticate someone: with their user-name and password, with two-factor authentication, and with a company-supplied device that you can trace. For most stuff, you should have two of those things. For critical things, you should have all three."[11]
>
> Alex Stamos
> Cybersecurity Expert

5.

Enforce Adaptive Access Policies

Context is everything when it comes to securing access. Implement granular policies for each application when possible to provide the right level of access by taking into account the user's role, location, network and trustworthiness of the device before granting application access.

6.

Continuously Monitor for Unusual Login Activity

Leverage user behavior analytics to flag and triage suspicious login activities such as access from a new location or a new device – which could be indicators of a potential breach. These alerts can be used to automatically block access, or generate a service-desk ticket for remediation or escalation.

In Conclusion

Social engineering and spear phishing are successful because they exploit the human element of an organization's security. There is no silver bullet for security, and cyber attacks are becoming increasingly common. Hence it is important to adopt and implement an "assume compromise" or a zero trust philosophy to security where credentials are assumed to be compromised and every access request needs to be authenticated with the appropriate level of security. IT security teams should carefully evaluate and invest in security technologies and create processes that empower their users to minimize the human element and strengthen the overall security of the organization.

Update Your Defense Beyond MFA With Duo

Organizations can defend against the impact of social and targeted phishing attacks by implementing conditional access policies that leverage contextual factors such as location and device posture in order to establish trust in users and their devices.

Duo's cloud-based security platform protects access to all applications, for any user and device, from anywhere. Duo is easy for administrators to roll out and for users to use, is cost effective and frictionless with other software.

Duo has simplified secure access to address identity and device risks with six critical capabilities:

1. Verify users' identities with secure and flexible **multi-factor authentication**[12] methods.

2. Deliver a consistent login experience with Duo's **single sign-on**[13] that provides centralized access to both on-premises and cloud applications.

3. Gain **visibility into every device**[14] and maintain a detailed inventory of all devices that access corporate applications.

4. Establish **device trust**[15] through health and posture checks for managed or unmanaged devices before granting application access.

5. Enforce **granular access policies**[16] to limit access to those users and devices that meet the organization's risk tolerance levels.

6. Monitor and detect risky login behavior using **Duo Trust Monitor**[17] or **export logs to your SIEM**[18] to remediate suspicious events such as new device enrollment for authentication or login from an unexpected location.

By layering Duo's strong user authentication (MFA) with device verification (Device Trust), administrators can implement strong access controls based on the risk profile of each application. For critical tools and applications, organizations can implement policies with Duo to limit access only from **corporate managed devices**[19] and require authentication using FIDO security keys, providing a high level of assurance for secure access. This helps prevent the use of compromised credentials and blocks unknown or risky devices from accessing corporate applications and sensitive data.

Adaptive policies[20] make it easy to adopt a principle of least-privileged access model. Organizations can ensure that the users are granted only the right level of access based on contextual factors such as the user's role and location, and the network being used. These layered controls can help prevent sophisticated attacks even when the user's password is phished and the user is tricked into approving an authentication request.

"Duo became the link we needed to make our security philosophy really work. We now know that if folks were downloading reports or manipulating data in a cloud application, that they were doing it from a safe device, and that their identity had been confirmed with MFA."[21]

Richard Hall
Senior Director IT Infrastructure and Operations, FinancialForce

Start your free 30-day trial at **duo.com/trial**.

References

[1] ***Microsoft report shows increasing sophistication of cyber threats***; Microsoft; Sept. 29, 2020

[2] ***Unpacking 2020's Verizon DBIR - Human Error and Greed Collide***; Duo Security; May 20, 2020

[3] ***Avoiding Social Engineering and Phishing Attacks***; Cybersecurity & Infrastructure Security Agency; Oct. 22, 2009

[4] ***For $500, this site promises the power to track a phone and intercept its texts***; The Verge; July 13, 2017

[5] ***New tool automates phishing attacks that bypass 2FA***; ZDNet; Jan. 9, 2019

[6] **What Is FIDO?**; FIDO Alliance

[7] **Security Keys and Duo**; Duo Security

[8] **WebAuthn.io**; Duo Security

[9] ***93% of Cloud Applications Aren't Enterprise-Ready***; Dark Reading; Feb. 23, 2018

[10] ***Information and App Overload Hurts Worker Productivity, Focus and Morale Worldwide, According to New Independent Survey***; BusinessWire; Sept. 18, 2017

[11] ***How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One***; Wired; Sept. 24, 2020

[12] **Two-Factor Authentication Methods**; Duo Security

[13] **Single Sign-On (SSO)**; Duo Security

[14] **Device Trust Insights**; Duo Security

[15] **Duo's Device Trust**; Duo Security

[16] **Duo's Adaptive Authentication Policies**; Duo Security

[17] ***Duo Trust Monitor Is Here to Make Risk Detection Easy***; Duo Security; Dec. 3, 2020

[18] ***Duo Log Sync: Sending Your Duo Logs to Your SIEM***; Duo Security; June 23, 2020

[19] **Duo Trusted Endpoints**; Duo Security; Jan. 14, 2021

[20] **Policy & Control**; Duo Security; Jan. 15, 2021

[21] **FinancialForce | Duo Case Study**; Duo Security