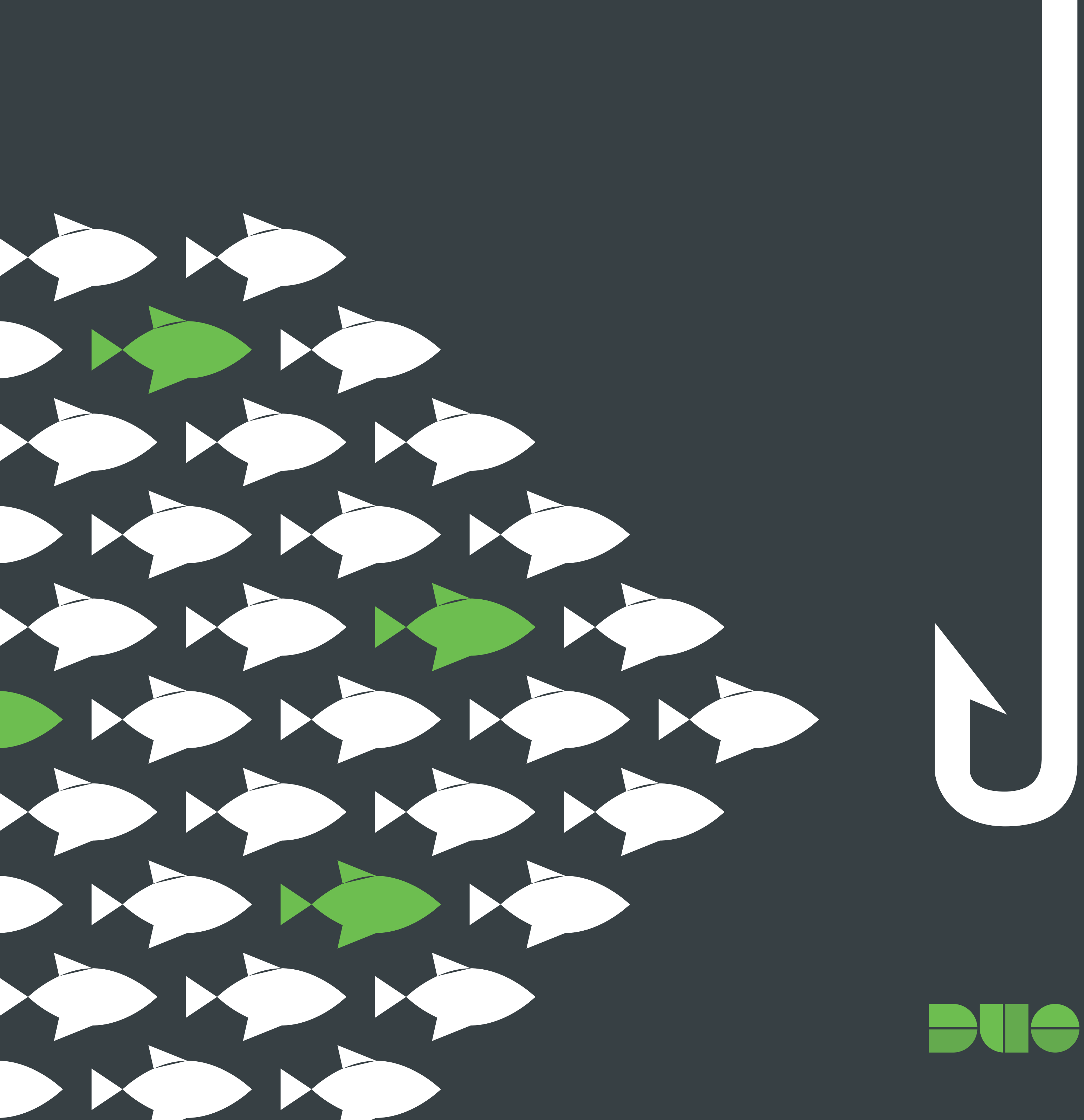
The Trouble With Phishing



AUTHOR
JORDAN WRIGHT

Phishing is one of the most common threats hitting organizations.

This guide details the problems around phishing, how it happens, and how Duo can be leveraged as a solution.

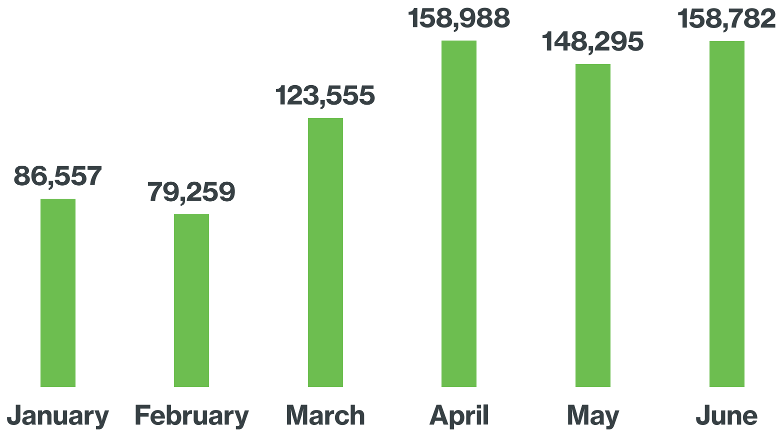
Phishing Affects Everyone

We've all seen the emails: someone shared a Google doc with us, our bank wants to verify our password, we've received an "important" attachment, you name it.

Phishing is common. It's common because it's ***easy***.

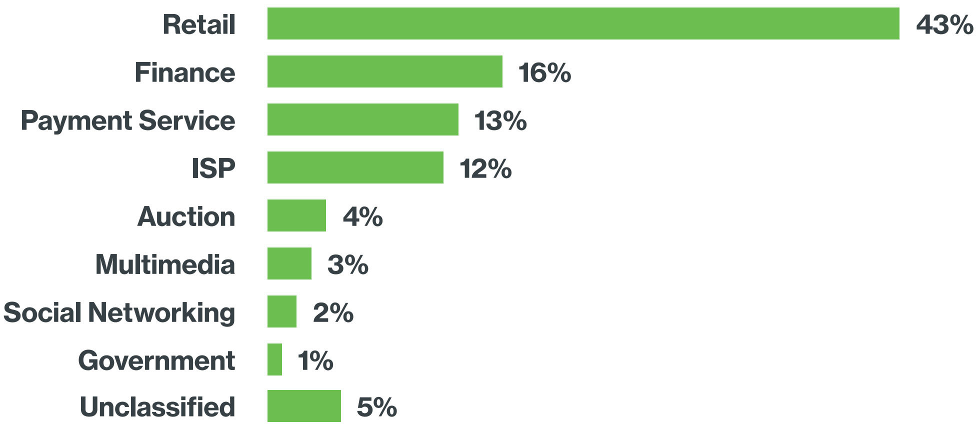
Not only is phishing common, but it's getting worse. In Q2 of 2016, the Anti-Phishing Working Group (APWG) **observed**[1] well over 460,000 unique phishing sites – a record for the most ever seen. That means **over 5,000 phishing sites were created every day.**

2016 PHISHING WEBSITES



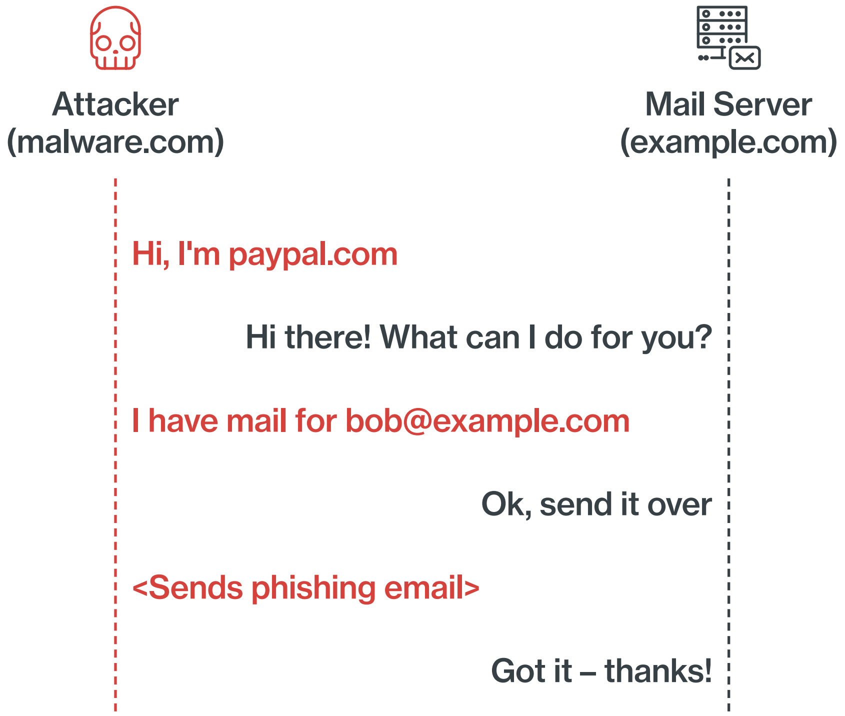
Phishing doesn't target everyone equally. APWG's report found that the industry most likely to be subjected to phishing attacks is retail/service, far ahead of other industries at 43 percent of all attacks. The financial industry follows at 16 percent.

PHISHING TARGETS BY INDUSTRY



How Does Phishing Actually Work?

In a nutshell, phishing works because email, like physical mail, is built to assume that the sender is who they claim to be. Without certain protections in place (which is true more often than not), an email exchange can look something like this:



Attacker (malware.com)

Mail Server (example.com)

Hi, I'm paypal.com

Hi there! What can I do for you?

I have mail for bob@example.com

Ok, send it over

<Sends phishing email>

Got it – thanks!

To detect and prevent spoofing, both the mail servers and mail senders need to be configured properly. This doesn't happen **most of the time**[2], which makes email spoofing possible.

It's important to note that **email addresses aren't always spoofed.** They don't have to be. Attackers can be tricky and do things like:

- Register a similar domain name (example: account-google.com as opposed to google.com)
- Use a domain that simply doesn't exist. (Yep! These are almost always delivered just fine.)

Now that we can send phishing emails, let's take a look at 3 of the most common phishing scenarios.

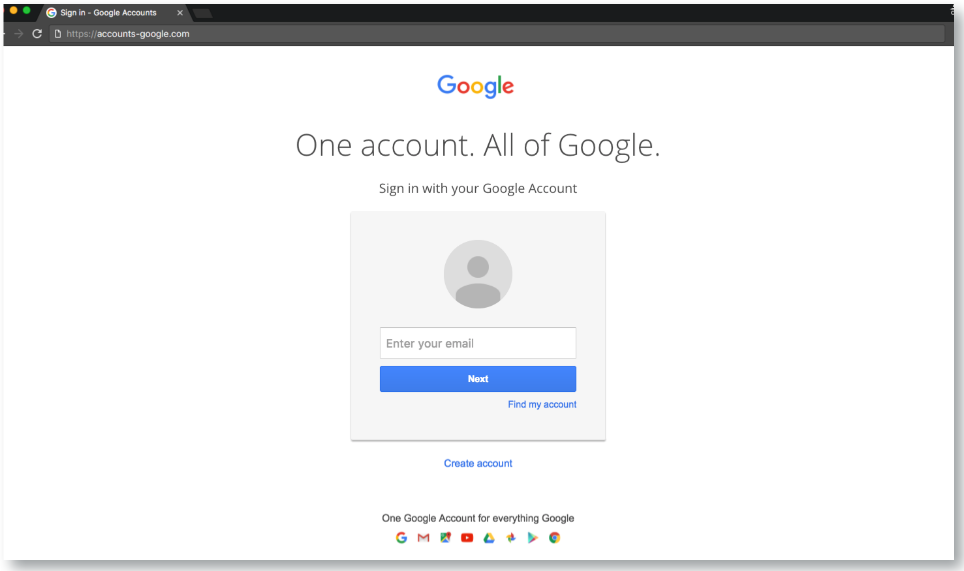
Anatomy of a Phishing Attack

SCENARIO 1

Credential Stealer

The most common attack is a basic credential stealer.

In this scenario, the attacker makes a convincing clone of an existing webpage and steals the credentials from the user. These credentials are then emailed to the attacker, or stored in a text file on the phishing site, waiting to be retrieved by the attacker.



Sign in - Google Accounts

https://accounts-google.com

Google

One account. All of Google.

Sign in with your Google Account

One Google Account for everything Google

SCENARIO 2

Exploit Kit

You don’t have to enter credentials to be affected by phishing. In fact, just clicking the link can mean game over.

Attackers have created reusable bits of code called “exploit kits” that are designed to exploit **known, old vulnerabilities** in browsers and browser plugins like Flash or Java. These exploit kits are then placed on websites so that anyone with an **outdated device** who visits the site can be compromised.

The user opens the email.

The user clicks the link in the email, unknowingly visiting a malicious page with an exploit kit.

The exploit kit compromises the user's out-of-date browser and downloads malware.

Once installed, the malware can steal passwords, install a backdoor or even encrypt the computer (ransomware).

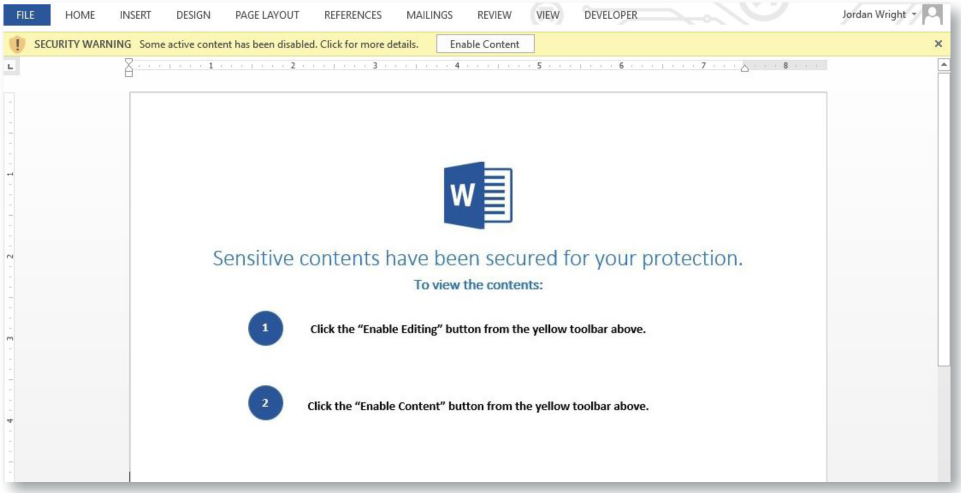
When malware is downloaded to the user’s computer, it knows where and how browsers store passwords, so it can quickly steal every credential saved to the browser. (This is another benefit to using a password manager!)

SCENARIO 3

Malicious Attachments

Malicious attachments come in all forms, such as Word documents, HTML files, or even executable programs (.exe, .jar, etc.).

The most common malicious attachments are Word (or any Microsoft Office) document files. In this case, the attachments contain code called **macros**. Malicious macros are typically bits of code designed to download and execute malware on a device.



SECURITY WARNING Some active content has been disabled. Click for more details.

Sensitive contents have been secured for your protection.

To view the contents:

1. Click the "Enable Editing" button from the yellow toolbar above.
2. Click the "Enable Content" button from the yellow toolbar above.

Microsoft knows letting macros run automatically is dangerous, so they prompt you to see if you want to execute the macros. Attackers, however, have gotten smart and try to trick you by making the content of the document say something like, "this document is encrypted for your protection," showing how to enable macros to "decrypt" the document. This allows the macro to execute, which downloads the malware.

The user opens the email and downloads the attachment.

The user opens the attachment and executes the malicious macros.

The macro downloads malware onto the user's computer.

Once installed, the malware can steal passwords, install a backdoor or even encrypt the computer (ransomware).

The Real Problem with Phishing

Many people think phishing is a credential problem. They believe they're safe as long as they didn't enter their credentials after clicking on the phishing link.

This isn't true.

Consider the exploit kit scenario. In that case, all you have to do is click the link and your browser (and device) are completely compromised. **Phishing is just as much a *device* problem as it is a credential problem.**

Phishing is Effective

31% of people click on phishing links.

17% of people enter credentials on phishing sites.

In addition to being easy, phishing is incredibly effective. We launched **Duo Insight** to let organizations see for themselves just how exposed they are to standard phishing tactics.

After our initial launch, we saw that **31% of people click the phishing links.** We also saw that **17% of users enter their credentials into the phishing site.**[3]

In addition to this, our ***2016 Trusted Access Report: Microsoft Edition***[4] found that as high as **72% of users are using an out-of-date plugin like Java**, making them vulnerable to exploit kits.

So, How Do We Fix It?

Ok, so phishing is effective. Organizations know this and they've used Duo Insight to prove it. The next question they are going to ask is "How do I *fix* it?" Traditionally, the solution most favored was *user awareness training*.

User awareness training can help reduce the impact from a phishing campaign, but it doesn't completely solve the problem since there will always be someone who clicks the link or has credentials stolen.

Let's look at each scenario and see how Duo can help:

SCENARIO 1

Credential Stealer

If credentials are stolen by attackers, they will try to re-use them to compromise the account.

The solution to this is to deploy Duo's **two-factor authentication** so credentials can't be re-used to access critical applications.

SCENARIO 2

Exploit Kits

Two-factor authentication doesn't help protect devices when it comes to exploit kits, so deploying two factor alone isn't enough to prevent phishing.

Duo's **Device Insight** helps to ensure devices are kept up to date so that exploit kits that target old or known vulnerabilities are mitigated.

SCENARIO 3

Malicious Attachments

Disabling macro execution via **Group Policy** is the recommended way to prevent against malicious macros. However, leveraging **Duo's Trusted Access platform** can be another line of defense when it comes to malicious attachments.

Even if account credentials are harvested from a compromised device, two-factor authentication prevents an attacker from gaining access to those accounts.

And, while an up-to-date device still could execute and run the malware attachment, it is less likely to be able to successfully leverage known vulnerabilities to do things like escalate its privileges.

Phishing Quick Stats

Q2 2016 saw a record

460,000

new phishing websites.

That's

5,000

new phishing websites *every day.*

31% of people click on phishing links.

17% of people enter credentials on phishing sites.

25% of Windows users are running an out-of-date version of Internet Explorer.

60% of Flash users are running an out-of-date version.

72% of Java users are running an out-of-date version.

References

[1] Anti-Phishing Working Group Q2 2016 Report

[2] Neither Snow Nor Rain Nor MITM . . . An Empirical Analysis of Email Delivery Security

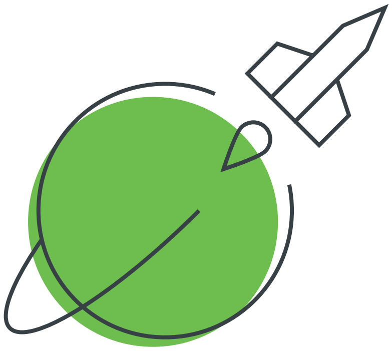
[3] So Your Users Clicked – Now What?

[4] 2016 Trusted Access Report: Microsoft Edition

Other Resources

Symantec Internet Security Threat Report Volume 21

OpenPhish Global Phishing Activity



DUO

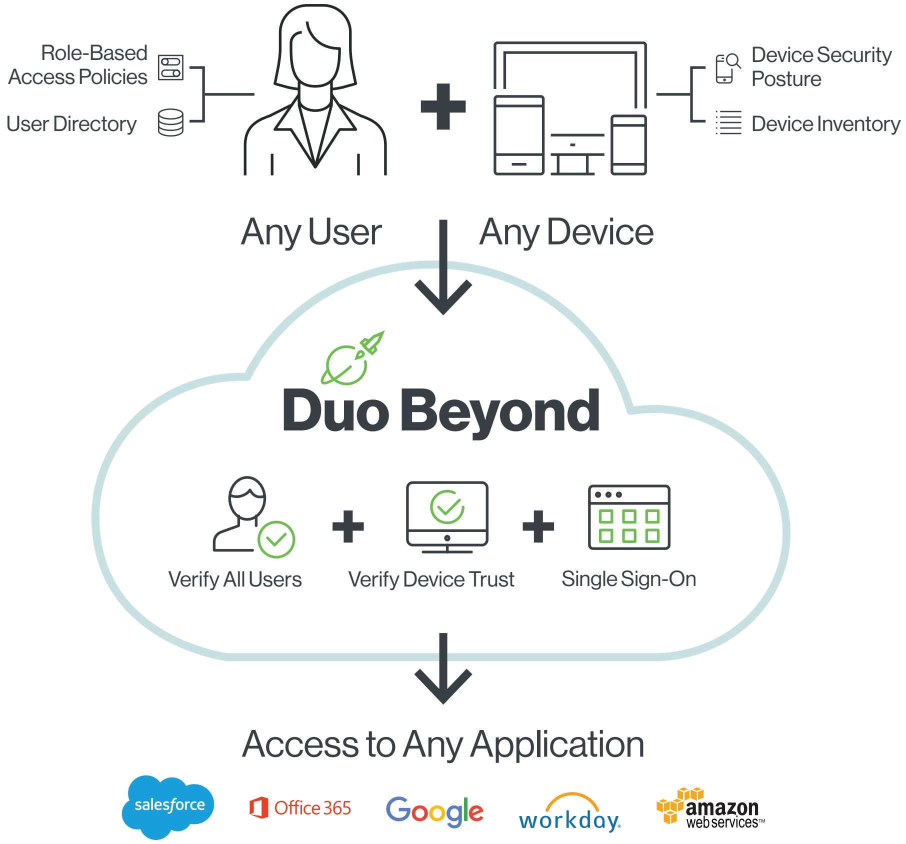
Beyond

Zero Trust for the Workforce

With **Duo Beyond**, you'll receive:

Full-featured two-factor authentication for every organization:

- Protect logins with **Duo's MFA**
- Insight into an overview of **device security hygiene**
- Manage Duo's solution with **Admin APIs**
- Duo's secure **single sign-on (SSO)** provides a consistent user login workflow across all applications
- Protect access to both **on-premises and cloud applications**



Role-Based Access Policies

User Directory

Any User + Any Device

Device Security Posture

Device Inventory

Duo Beyond

Verify All Users + Verify Device Trust + Single Sign-On

Access to Any Application

Essential access security suite to address cloud, BYOD and mobile risks:

- Complete visibility into both mobile and desktops, including **corporate-managed and unmanaged** (personally-owned) devices to support BYOD policies
  - Mobile device breakdown with visibility into enabled **security features and tampered or unencrypted devices**
- Enforce rules on who can **access which applications, under what conditions** (adaptive authentication)
- Enforce a policy to **allow only managed devices** access to sensitive applications
- Provide modern **remote access to multi-cloud environments** (on-premises, Azure, AWS, Google Cloud Platform) while enforcing zero-trust security principles
- **Notify users** to update their devices based on device access policies
- Full-featured dashboards and custom reports for **compliance audits** and ease of administrative management

Learn more about Duo Beyond in our **documentation**.