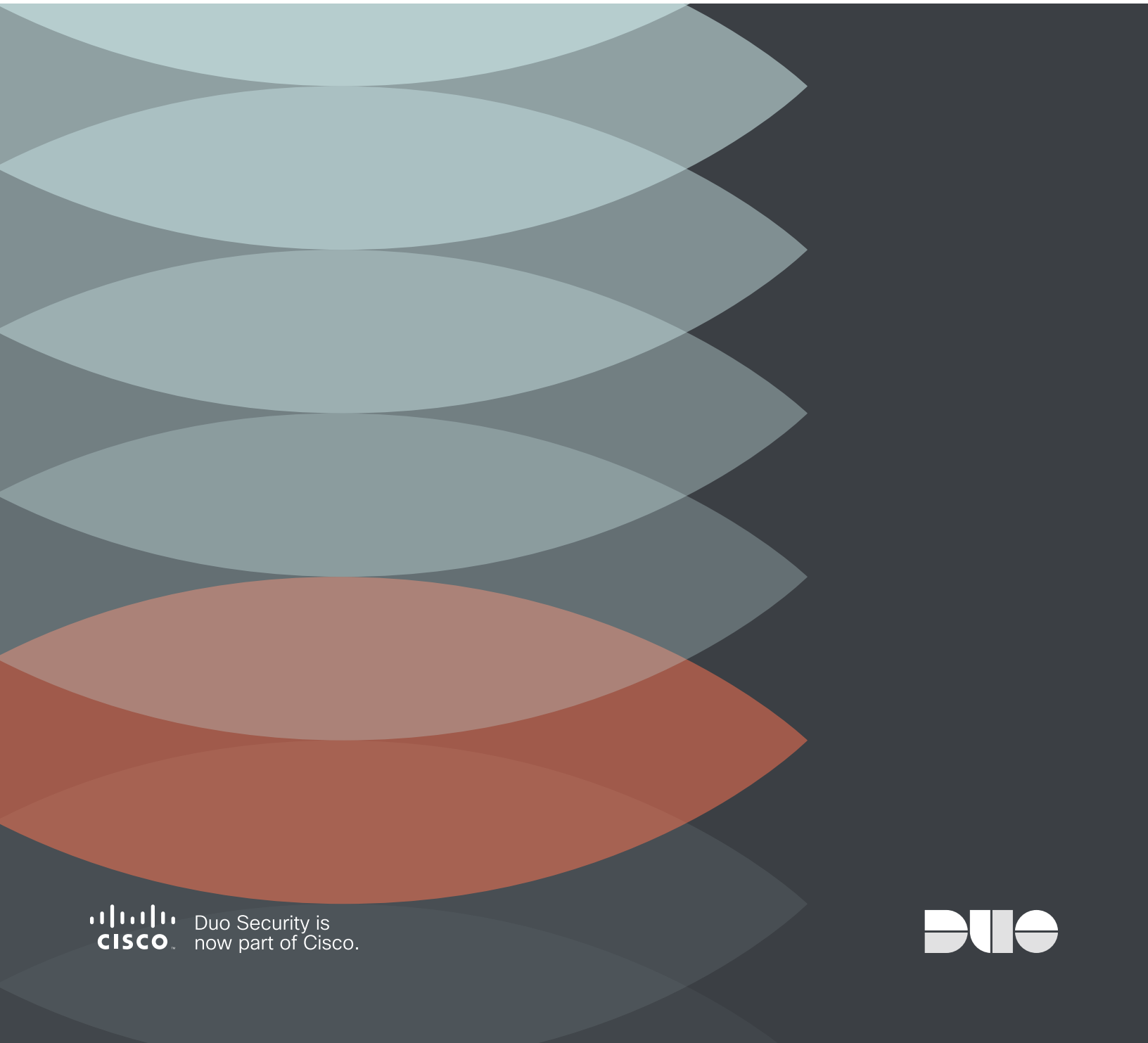
# Phishing

## A Modern Guide to an Age-Old Problem



Duo Security is now part of Cisco.

# Phishing

## A Modern Guide to an Age-Old Problem

# Phishing the New Enterprise

# Phishing is a low-effort, successful method for attackers seeking unauthorized access to your organization's data.

Organizations comprise people, and those people's behaviors are driving change at the consumer level and at the enterprise level. They use smartphones, tablets, smartwatches and more to meld work and personal computing. They're increasingly remote, distributed and working odd hours, from different locations – communication, data and apps are expected to be available, on demand.

As a result, staying competitive in today's market demands business agility and adaptation — and development and support for the technology that enables it — cloud computing, web applications, mobile and connected devices.

Yet, it's so easy to exploit this new enterprise model for malicious gain. Phishing is a low-effort, successful method for attackers seeking unauthorized access to your organization's data.

With a password, it's trivial for an attacker to gain remote access to your company's network where they can move laterally within – undetected and undeterred. This type of attack bypasses traditional security measures (like firewalls) that focus on protecting the perimeter of your network, but fail to protect the inside.

## This guide gives you a look into:

- How phishing works, how it has evolved, and the new tactics used to appear legitimate to users
- Statistics into who and what industries phishers are targeting, what people click on the most, and what is being stolen
- What to look out for, tips for both admins and users on how to protect against phishing, and how a zero-trust security model can help protect your organization

Protecting your network both externally and internally requires more controls than a traditional perimeter security model and must rely on trust in user identity and device health. This will help secure the new "identity-based perimeter."

1.0

# What is Phishing?

## Phishing is an attempt to deceive users in order to steal sensitive information from them via emails, telephone or text message.

### Social Engineering

Phishing is a form of **social engineering** - the act of deception, or taking advantage of a user's trust to convince them to reveal sensitive information.

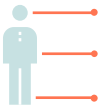
### Spear Phishing

Spear phishing is a type of phishing attack that targets a specific individual or set of individuals. Attackers may do research on their targets via social media networks and publicly available information online, using the data to craft a credible message to convince victims to click, download or give away additional, non-public information.

# Information Targeted in Phishing Attempts

**Usernames and passwords** that can be used to log into personal and work accounts

**Email addresses** of colleagues or family and friends that can be used to send more convincing phishing emails



**Personally identifiable information** like names, physical addresses, birthdates, Social Security Numbers, etc. that can be used for identity theft

**Confidential company information**, like details about mergers and acquisitions, research and development, and any other information that could be used to influence stock trading or for competitive gain

**Financial data** like credit card numbers, tax information or W2s that could be used to commit tax fraud and steal money

**Phone numbers** that can be used to bypass two-factor authentication, as well as used to deliver SMS-based phishing campaigns

**Medical records or health insurance information** like insurance policy IDs that could be used to commit healthcare insurance fraud

2.0

# How Phishing Works

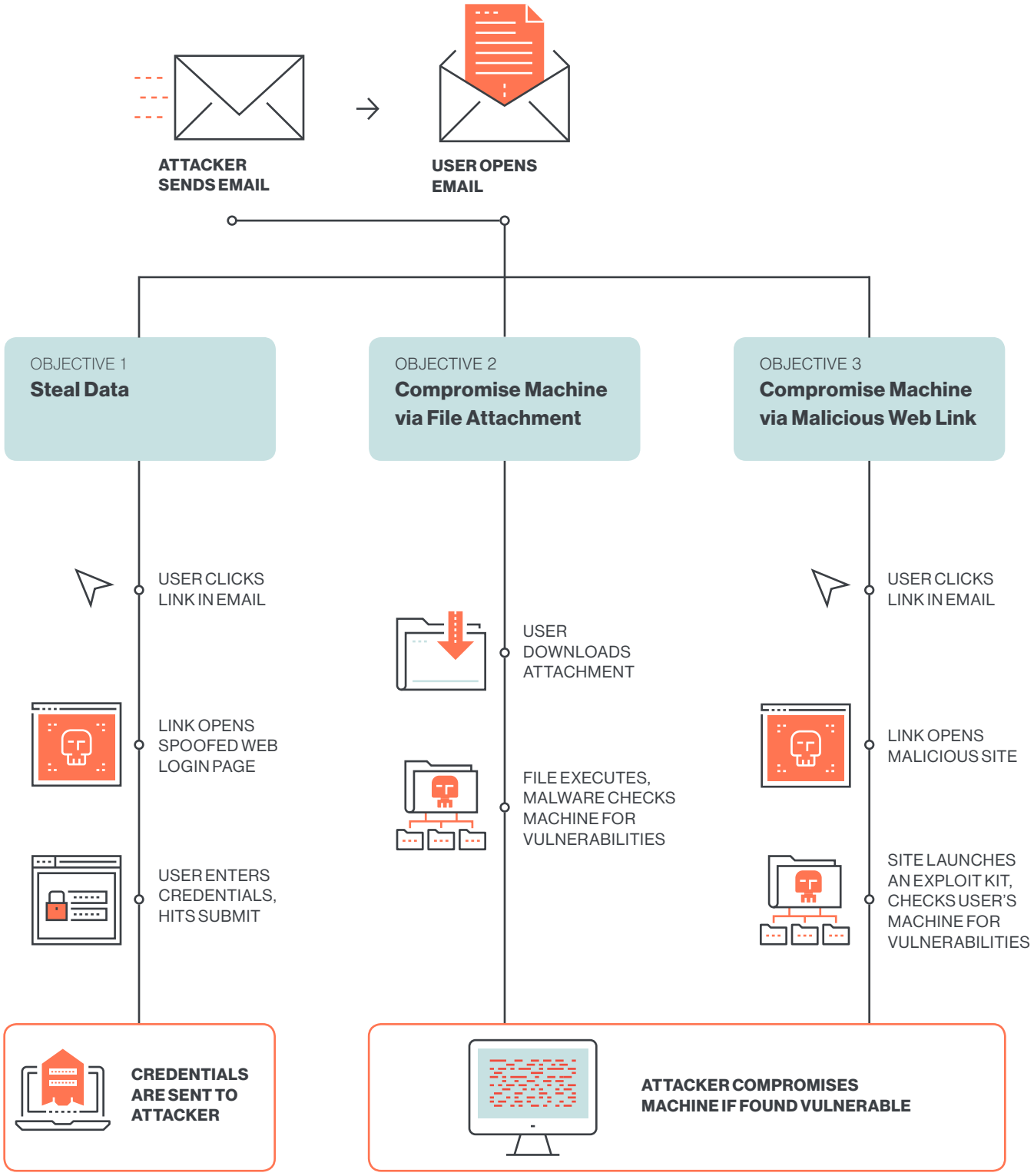
Phishing methods and objectives vary from credential and data theft to malware infection and machine compromise. Understanding the choose-your-own-adventure workflow sheds light on what preventative measures you need to take to protect against phishing consequences.

## Focusing on phishing emails, their methods typically involve:

- **Send email to user**
- **Steal data by persuading user to:**
    - Send them information directly
    - Click on a link, visit spoofed site, then enter username and password
    - Download an email attachment which executes malware
    - Visit a malicious website hosting an exploit kit that executes malware

# Different Phishing Methods

The objectives and methods of phishing attempts may vary - and understanding how malware is spread and credentials are stolen is half the battle.



3.0

# Protecting Against Phishing

## For IT Administrators

### Implement and require two-factor authentication.

That way, even if your users' passwords are compromised through a phishing attack, their accounts will still be protected by a second factor of authentication. Attackers can't log in without possession of their physical device, like a phone or security token.

The most secure method requires using a **U2F (Universal 2nd Factor)** compliant, USB device plugged into users' computers, allowing them to easily tap it to quickly and securely log in.

### Encourage users to update devices on timely basis.

In *Different Phishing Methods* (previous page), the user downloads a malicious attachment, which checks their device for vulnerabilities before compromising it.

Devices running older versions of software, without any security features enabled, are more likely to be affected by publicly-known vulnerabilities – which leaves them prone to a compromise.

### Get visibility into the security health of devices accessing your network.

Many users are using their personal smartphones and laptops to log into your organization's resources, from different networks and at all hours. Use an endpoint security solution to gain insight into the security health of every device.

### Get visibility into the personal vs. corporate-owned devices on your network.

Personal devices in the workplace may have multiple work and personal accounts, as the line between the two has blurred. BYOD can introduce risks, but your team can support it by using an endpoint solution to identify personal vs. corporate devices, and strengthening access security policies to require more stringent security checks for personal devices accessing work applications.

# For Users

## Type in URLs yourself; don't click on links in emails.

Web addresses may not be what they appear in your email messages – better to type in the domain name yourself before entering any sensitive information into any web forms.

## Turn on two-factor authentication (2FA) for every account.

If you're able to, use a free **authentication mobile app**, and set up **push authentication-based 2FA** for all of your online accounts to protect against unauthorized access via phishing. Or, use **passcode-based** methods if that's what is offered (set up your mobile app to generate unique passcodes, then enter them into your login screen).

## Beware of certain social cues, urgent requests, and gift or money offers.

Messages that appear to be urgent requests for either immediate payment, updates to your account, password changes, etc. play on the reactive emotional response of a user to get information from them quickly.

## Beware of social media, entertainment or reward scams.

Attacks targeting social media platforms have nearly tripled since last year, according to **PhishLabs**. These types of scams are leveraging the inherent trust between users and a platform or brand. By targeting employees that mix personal and business practices, scammers are hoping that employees may lower their guard for a message that appeals to them on a personal level.

## Verify the sender in person or via a different channel of communication.

If you're able to, verify that the sender actually sent you the message in question by asking them in person or over a different messaging service, or call them. Sometimes those methods can also be compromised or phished, so if you're still unsure, send the message to your IT or security team for review.

## Check for and run updates; use software that updates automatically whenever possible.

Keeping your software and devices up to date is one way to protect against malware compromises and data theft as the result of phishing. Do them often and on a timely basis.

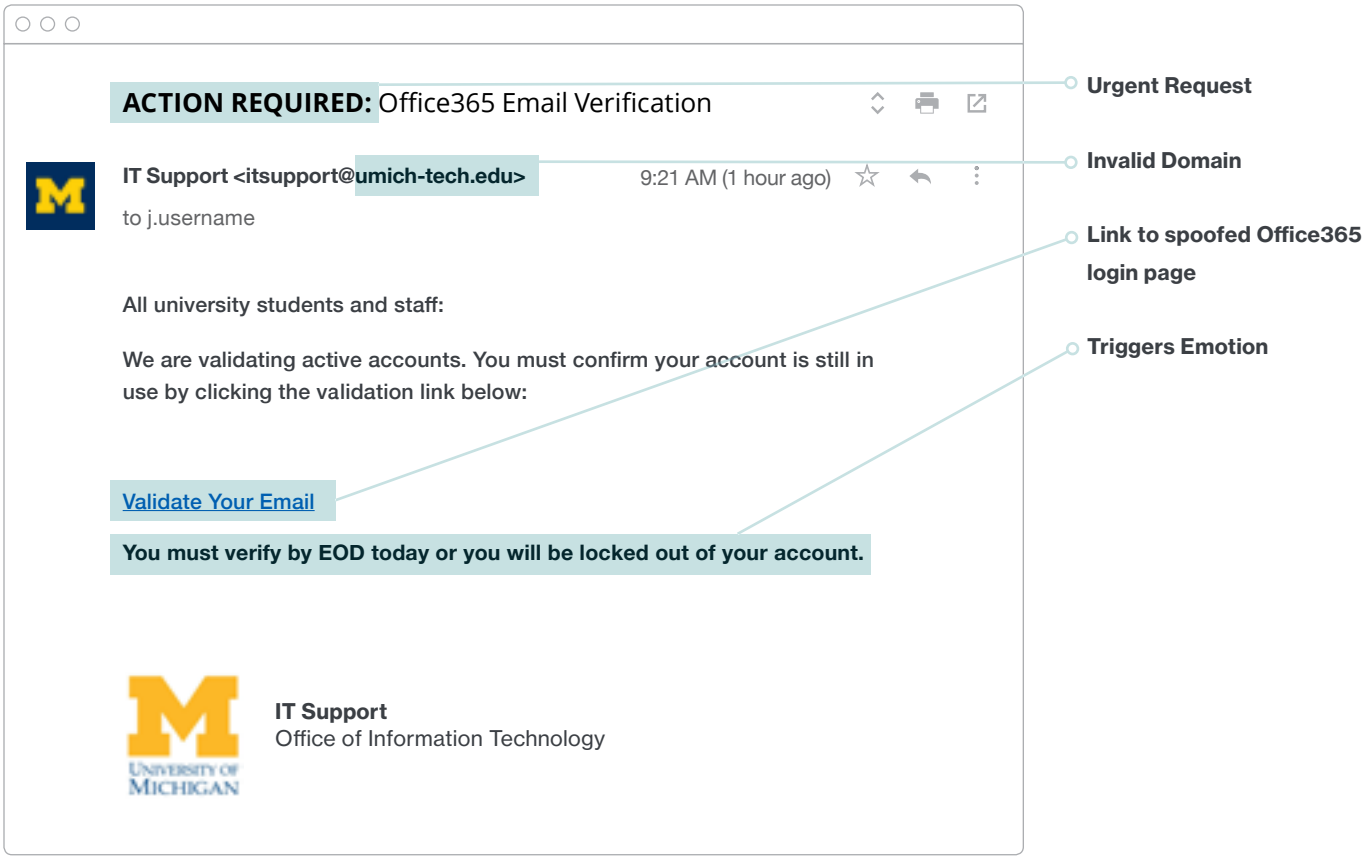
4.0

# What to Look Out For

A quick list of phishing message identifiers for users to reference:

- Impersonates reputable organizations
- Triggers an emotion
- Urgent request
- Asks for personal information
- Offers gifts or money
- Poor spelling and grammar
- Mismatched URLs

## Phishing Example



# Modern Phishing Tactics

Nowadays, not all phishing messages are easy to spot, and attackers have discovered ways to evade the more obvious indicators. One way users are trained to identify illegitimate web login pages is to check for an unencrypted connection (HTTP) – which, if you're using **Google Chrome**, can easily be identified in the web address bar – a small red exclamation mark icon indicates a non-HTTPS website, marking it as not secure or dangerous.

However, there are now reports of phishing attempts using web pages that are encrypted, displaying the green lock icon in your address bar, as reported by **Krebs on Security**, which can lead to confusion for users taught to trust the icon. The icon is not an indication that the website you're visiting is legitimately the site you intended to visit.

According to PhishLabs, by the end of 2017, nearly one-third of all phishing sites were located on HTTPS domains, up from only five percent at the end of 2016. This exponential growth shows how quickly phishers have adopted site encryption to use to their advantage.

> **"Phishers are preying on the common misconception that HTTPS means a site is legitimate or trustworthy."**
>
> **—**
> **PhishLabs**

Plus, the trend toward HTTPS-encrypted sites is seen in major browser vendor actions – in July 2018, **Google Chrome** will mark all HTTP sites as not secure. About 81 percent of the top 100 sites on the web default to HTTPS, according to **The Verge**. It's clear that as the majority of web traffic shifts to encrypted sites, phishing sites will follow.


Secure
Info or Not secure
Not secure or Dangerous

# Phishing Kits

A phishing kit is a bundle of site resources that can make campaigns more efficient and reusable, enabling non-technical phishers to easily create spoofed websites and launch a phishing attack. For more information about phishing kits, read ***Phish in a Barrel: Hunting and Analyzing Phishing Kits at Scale***.

Google's report analyzed a sample of 10,037 phishing kits and about 3.8 million credentials that belonged to victims of the kits. They found that the most popular phishing kit was used by almost 3,000 attackers to steal 1.4 million credentials – this kit included a website that emulated Gmail, Yahoo and Hotmail logins. By far, Gmail was the most popular email provider used by phishers as exfiltration points to receive stolen credentials (72.3 percent).

The top phishing kits impersonate several other brands, including file storage services (Dropbox, Office 365), webmail providers (Workspace Webmail, AOL) and business services (Docusign, ZoomInfo).

Phishing kits collect not only credentials, but also additional information such as geolocation data, secret questions and device-related details. This type of info can be used to bypass login challenges for services that attempt to detect suspicious login attempts.

**The most popular phishing kit was used by nearly**

**3000**

ATTACKERS

**Exposing**

**1.4 million**

USER CREDENTIALS

# Social Media

As mentioned earlier, phishing attempts on social media platforms have nearly tripled since last year. All of that hard-earned brand trust built up over the years by marketing/public relations teams is being leveraged to a scammer's advantage - seeing the logo or name of a trusted company can be enough to convince or momentarily fool a user into clicking on a link or giving away personal information.

Another 55 percent of social media attacks that impersonated customer-support accounts were targeting customers of financial services companies, according to Proofpoint's 2018 ***The Human Factor*** report.

About a third of social media scams use clickbait-type links to get users to visit video streaming and movie download sites, as reported by Proofpoint. The scammers then hijacked users' computers and browsers for cryptocurrency mining, allowing them to use their central processing unit (CPU) to steal cryptocurrency online.

**Seeing the logo of a trusted company can be enough to momentarily fool a user into clicking on a link or giving away personal information.**

5.0

# The Impact of Real-World Phishing

## Phishing Statistics & Trends

At the end of 2017, the *Anti-Phishing Working Group (APWG) Phishing Activity Trends Report* revealed a growth in phishing targeting software as a service and webmail providers. They also saw an increase in attacks on financial and banking, as well as cloud storage and file-sharing sites.

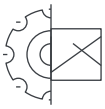
They actually saw a five percent decrease in the number of unique phishing sites from the third quarter of 2017 to the fourth quarter.

# Who is Being Targeted?

In a study of phishing across different industry sectors in the fourth quarter of 2017, MarkMonitor found increases in attacks on financial/banking organizations and file hosting/sharing sites.

**42%**

**Payment Services**



**16%**

**SaaS & Webmail**

**15%**

**Financial Institutions**

**11%**

**Cloud Storage & Hosting**

**3%**

**Retail & eCommerce**

**3%**

**Telecom**

**3%**

**Social Media**

Source: **APWG's Phishing Activity Trend Report, 4th Quarter, 2017**

According to PhishLabs' ***2018 Phishing Trends and Intelligence (PTI) Report***, email and online services (26 percent of all attacks) bumped financial institutions as the top phishing target (21 percent). The major increase was driven almost exclusively by a concentrated rise in attacks impersonating Microsoft Office 365 login pages. PhishLabs analyzed more than 1.3 million malicious phishing sites in 2017 on nearly 300,000 unique domains.

The number of phishing attacks against the software as a service (SaaS) industry grew steadily throughout 2017 at more than 237%, showing major growth from five percent in 2016. These attacks mainly targeted Adobe and DocuSign, applications used by enterprises, and shows a shift from targeting mostly individuals to targeting organizations with phishing attempts.

# Who is Clicking on Phishing Campaigns?

The click rates of phishing emails were the highest in automotive, aerospace, defense and commercial banking - all associated with high Dropbox click rates, according to a Proofpoint 2018 report on ***The Human Factor***.

## Clicks While Running Older Systems

The ***2018 Duo Trusted Access Report*** revealed that more than half of campaigns involved one out-of-date device (64 percent), in addition to capturing at least one set of user credentials (62 percent).

**62%** of campaigns captured at least **one set of user credentials**

**64%** of campaigns involved at least **one out-of-date device**

Source: Duo Security

**Why is this a problem?** When an attacker sends a phishing email with a malicious link, it can often lead to a spoofed login page that captures usernames and passwords – but sometimes it can also lead to a web page hosting an exploit kit or malware that leverages older, unpatched operating systems (OS).

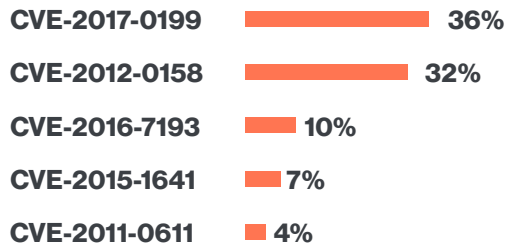
Looking back at 2017, the high-severity Microsoft Windows OS vulnerability, **CVE-2017-0143**, was said to be used by the NSA as a hacking tool to gather intelligence. Known as EternalBlue, the vulnerability led to the spread of WannaCry and (Not)Petya ransomware, due to the fact that many had not yet applied the Microsoft patch that protected against the exploit.

***Sophos' 2018 Malware Forecast report* (PDF)** found that there's a new CVE that has emerged as the most exploited vulnerability – CVE-2017-0199 accounts for 36 percent of all attempted attacks. CVE-2017-0199 affects multiple versions of Microsoft Office, allowing for the execution of arbitrary code via a specially crafted Word document.

Meanwhile, the second-most exploited vulnerability, CVE-2012-0158, accounts for 32 percent of attacks. CVE-2012-0158 was patched by Microsoft in 2012, but is still used frequently by attackers, indicating that it's been more than five years and many still haven't patched for the bug. The flaw affects Windows common controls in several Microsoft applications, allowing for remote code execution.

Sophos did not release any methodology or sample size information in their report.

TOP VULNERABILITIES EXPLOITED IN ATTACKS




Source: **Sophos**

# What Are People Clicking On?

Once users open phishing emails, what are they most frequently clicking on? Wombat Security's ***2018 State of the Phish*** report reported high click rates on (sample size of 1,550):

**89%** **Corporate Email Improvements**

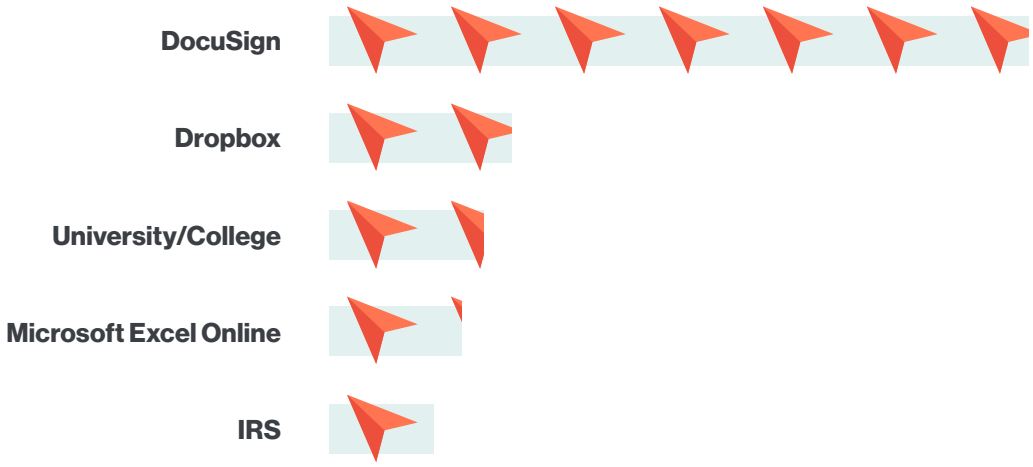
**86%** **Online Shopping Security Updates**

Source: Wombat

The report saw a slight increase in click rates on commercial emails – that is, business-related emails that aren't organization-specific, including shipping confirmations and wire transfer requests.

Proofpoint found that users were most frequently clicking through on DocuSign and Dropbox phishing campaigns (two applications used by enterprises), as well as phishing campaigns sent in universities.

**AVERAGE CLICK RATES:** TOP 5 LURES




Source: Proofpoint

# What is Being Stolen?

Google and the University of California conducted a longitudinal study and found that 90 percent of Google users do not have two-factor authentication (also commonly referred to as two-step verification) enabled on their accounts.

Additionally, only 3.1 percent enable two-factor authentication after they've recovered their accounts following a compromise, showing a lack of user education and knowledge in how to stop further attacks, as noted in Google's ***Data Breaches, Phishing or Malware? Understanding the Risks of Stolen Credentials***.

Proofpoint also found that, overall, around 60% of cloud service users, including 37% of privileged users, did not have a password policy or multi-factor authentication enforced, according to ***The Human Factor 2018*** report.

As a result, many are being compromised. And once compromised, what do the phishers steal? Credentials, financial data, and more.

**9/10** **Google users do not have two factor enabled.**

Source: Google

## Credential Theft Trends

After getting access to their email inbox (or other accounts), phishers will often search for financial data and other credentials related to third-party services. For example, an attacker could use an email address to reset passwords on a social media site, like Twitter, or an online shopping site, like Amazon. Then, with access to the user's email, they can change the password and subsequently maintain complete control over their accounts.

This same scenario can play out with other types of accounts, including work-related applications that contain confidential and proprietary company information - from human resources to financial data.

On average, 12 percent of phishing simulation participants entered in credentials into a fake login web page, while another 62 percent of phishing simulation campaigns captured at least on set of user credentials, according to the ***2018 Duo Trusted Access Report***. These findings came from the analysis of 7,483 phishing simulation campaigns conducted from mid-2017 to April 2018 on more than 230,000 recipients.

PHISHING CAMPAIGN SIMULATION RESULTS

**43%**
Opened the email

**23%**
Clicked the link

**12%**
Entered credentials

**10%**
Had out-of-date browsers

**15%**
Had out-of-date operating systems

Source: Duo Security

## Tax Fraud Trends

Phishing topped the list of the U.S. Internal Revenue Service (IRS)'s ***Dirty Dozen*** information campaign intended to educate tax filers on social engineering and other types of fraud during the 2018 tax season. It's important to note that the IRS will never contact anyone unsolicited by telephone, email or social media, which can help people narrow down where the risks lie.

The latest phishing scheme involves stealing client data directly from tax professionals and filing fraudulent tax returns. Then the criminals will use victim's real bank accounts to directly deposit refunds. Finally, the criminals will contact victims and attempt to reclaim the refund, falsely claiming to be from a collection agency or representing the IRS.

In another email scam, criminals pose as a trusted person or organization (like tax, payroll or human resources professionals). Then they get access to their email account and send mass emails to their contacts, attempting to collect money, passwords, Social Security Numbers (SSNs) and more.

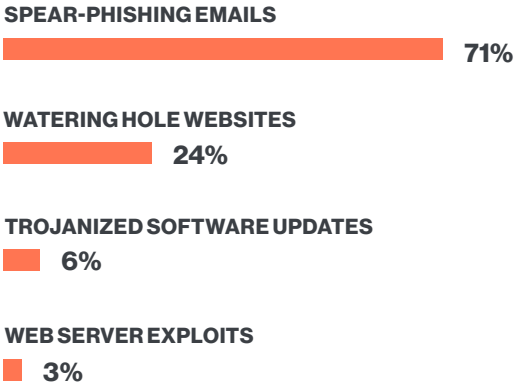
Some email phishing scams impersonating the IRS offer victims a generous tax return – playing on the human motivator of greed to get them to reply with their PIN numbers, passwords, bank account information, etc., as reported by **CSO Online**.

## Malware Infection Trends

Phishers don't just steal credentials and financial data, however, they also use phishing tactics to send links to malicious websites and malware attachments to their targets, as mentioned earlier.

According to Symantec's ***2018 Internet Security Threat Report*** (ISTR), spear phishing is the top malware infection vector – used by 71 percent of organized groups in 2017. Their report revealed that only 27 percent of attack groups have used zero-day vulnerabilities (undisclosed, new bugs) to infect targets. This shows that phishing is still more effective at infecting users than trying to find new software flaws to exploit.

TOP MALWARE INFECTION VECTORS




Source: Symantec

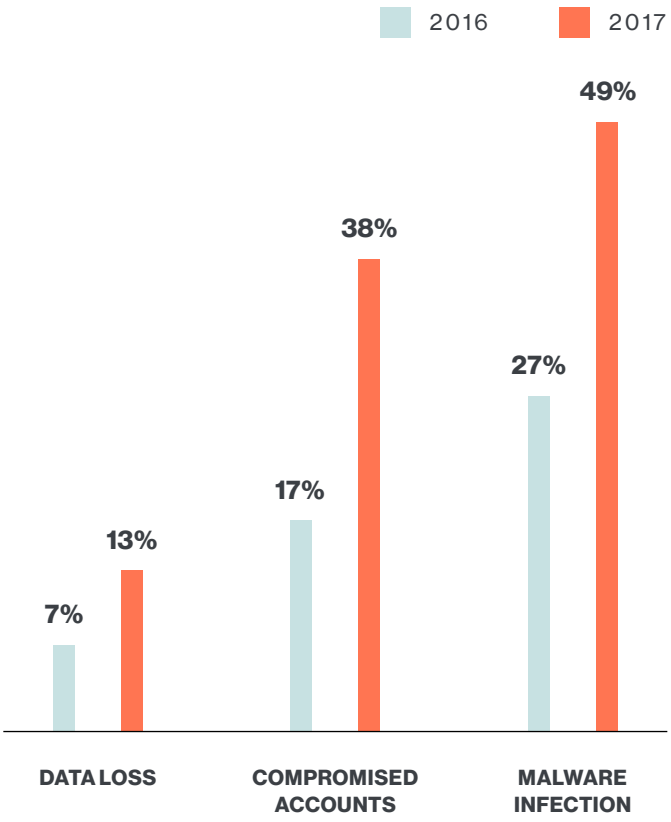
Wombat's ***2018 State of the Phish*** report also found that malware infection has risen from 27 percent in 2016 to 49 percent in 2018, according to a survey that asked participants about what effect phishing has had on their organizations. The report also found that compromised accounts (36 percent, up from 17 percent) and loss of data were (13 percent, up from 7 percent) counted among other consequences of phishing.

Wombat's quarterly surveys included an analysis of more than 10,000 responses from information security professionals.

The types of malware that infect victims via phishing can range from ransomware (data may be held hostage until victims pay criminals a ransom; sometimes the data is destroyed anyway) to Trojans and keyloggers that can track and steal data, including usernames and passwords.

Financial Trojans don't just steal banking credentials, however. In 2017, a Trojan called Dridex was seen checking device software for accounting software, then enabling remote access to infected networks in order to carry out larger fraud against these targets, according to **Symantec**.

WHAT PHISHING IMPACTS HAVE YOU EXPERIENCED?




Source: Wombat

## 6.0

# Summary

Here's a high-level summary of the top trends in phishing from the data presented in this report:

**Modern phishing tactics are advancing to both fool users and collect more data to ensure the success of an account compromise**

**Some of the most exploited vulnerabilities were patched more than five years ago, yet still are successful today**

**Phishing volume has increased, including attacks against SaaS and webmail providers, financial and banking and file hosting and sharing sites**

**Phishing is the top malware infection vector, outpacing zero-day vulnerabilities**

**Many users click on malicious links or attachments, using out-of-date devices that leave them susceptible to known vulnerabilities**

## Modern phishing tactics are advancing to both fool users and collect more data to ensure the success of an account compromise.

All of these trends point toward the effects of phishing – compromised accounts and networks, data loss, malware infection, fraud, etc.

Phishing lets attackers easily bypass traditional perimeter-based controls like firewalls by allowing them to remotely log in as legitimate users, undetected on your network.

Data, applications and resources are all hosted and accessible on the cloud. Users will continue to use their device(s) of choice, logging into resources from untrusted networks as they travel and work remotely. As a result, **some say identity is the new perimeter** – requiring effective security controls to address risks around users and their devices.

This new security model addresses new identity risks and ensures that the traffic inside your network is no more trusted than the traffic coming from outside of it.

7.0

# Establishing Trust With Duo Beyond

By establishing trust in your users and their devices before granting them access, you can protect against the impact of phishing attacks.

At Duo, we've simplified the path to secure access with Duo Beyond. Here are the steps we can help you take along your journey:

1

## Establish Trust in User Identities

Verify the identity of all of your users with effective, strong **two-factor authentication** before granting access to corporate applications and resources.

2

## Extend Visibility Into Users' Devices & Activity

**Gain visibility** into every device that is used to access corporate applications, whether or not the device is corporate-managed, and without the use of device management agents.

3

## Ensure User Device Trustworthiness

Inspect all devices used to access corporate applications and resources in real-time, at the time of access, to **determine their security posture** and trustworthiness.

4

## Enforce Risk-Based & Adaptive Access Policies

Protect every application by **defining policies** that limit access to those users and devices that meet the organization's risk tolerance levels.

5

## Enable Secure Connections to All Applications

Grant users secure access to all protected applications (on-premises or cloud-based) through a uniform, **frictionless interface** accessible from anywhere.

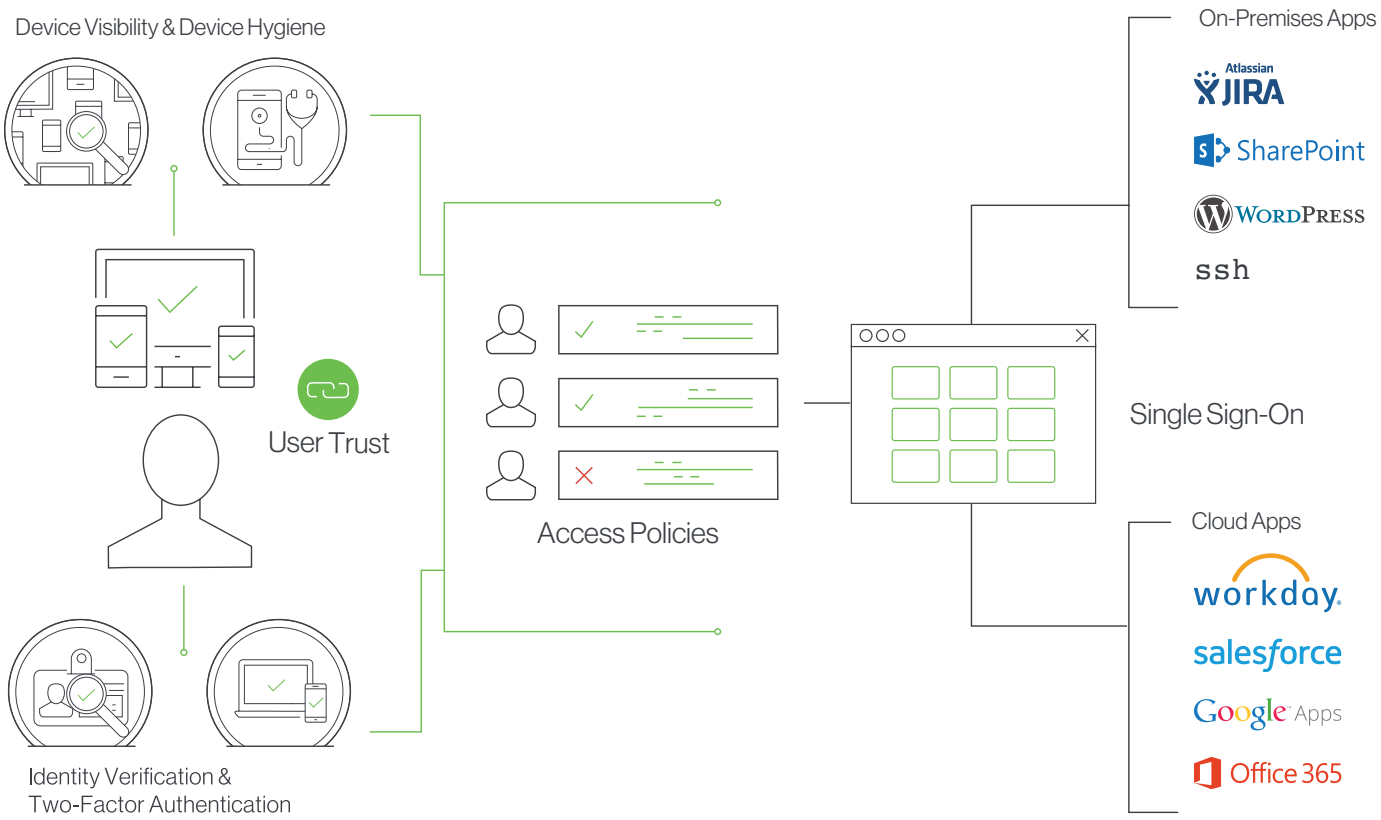
## Secure Access

**By combining different factors – trust in your users' identity and trust in their devices, all enforced by risk-based access policies – you can ensure your users are granted secure access to your applications.**

# Beyond

Trusted Users. Trusted Devices. Every Application.

Duo Beyond has made the BeyondCorp journey possible for companies such as **KAYAK**, allowing them to tighten their security controls both inside and outside the perimeter, and saving them months or years of effort piecing together their own solutions.




## Learn more about Duo Beyond and try it out free for 30 days at duo.com/beyond.

**ABOUT DUO SECURITY**

Duo Security helps defend organizations against data breaches by making security easy and effective. Duo Beyond enables organizations to provide trusted access to all of their critical applications, for any user, from anywhere, and with any device. The company is a trusted partner to more than 10,000 customers globally, including Dresser-Rand, Etsy, Facebook, K-Swiss, Random House, Yelp, Zillow, Paramount Pictures, and more. Founded in Michigan, Duo has offices in Ann Arbor and Detroit, as well as growing hubs in Austin, Texas; San Mateo, California; and London, UK. Visit **duo.com** to find out more.