

2018

Phishing and Fraud Report

ATTACKS PEAK DURING THE HOLIDAYS

Authors: Ray Pompon, Debbie Walkowski, and Sara Boddy



Michael Levin, CEO & Founder, Center for Information Security Awareness – CFISA.com

CONTRIBUTORS
Justin Shattuck

DATA CONTRIBUTORS
F5 Security Operation Center for WebSafe, Webroot

WEBROOT
Smarter Cybersecurity®

Table of Contents

EXECUTIVE SUMMARY	4
INTRODUCTION	6
PHISHING: THE EASIEST WAY TO GET YOUR DATA	7
HOW PHISHING WORKS	9
Impersonation is a Key Tactic	10
Common Phishing Lures	11
Top 10 Impersonated Organizations	17
MALWARE ATTACKS THAT TARGET CREDENTIALS	20
How Malware Steals Credentials	21
HOW SCAMMERS USE STOLEN ACCESS TO LOOT APPS	22
Stolen Credentials Lead to Fraudulent Transactions	24
DEFENDING AGAINST PHISHING AND FRAUD	25
Teaching Users to Resist Phishing Lures	25
Things to Watch Out For	26
Technological Defenses	28
How to Distinguish Between a Legitimate User and a Bot that Uses Stolen Credentials	30
Inspect Encrypted Traffic for Malware	32
PHISHING INCIDENT RESPONSE	33
CONCLUSION	35

Table of Figures

<i>FIGURE 1: F5 Security Operations Center data shows fraud incidents jump significantly in October, November, and December</i>	6
<i>FIGURE 2: The majority of fraud sites shut down by F5's Security Operations Center are phishing sites</i>	8
<i>FIGURE 3: Phishers generally follow this three-step process to concoct their phishing schemes</i>	10
<i>FIGURE 4: Phishing emails regarding bills or invoices often contain malicious links and documents</i>	12
<i>FIGURE 5: Fake Facebook phishing email—evidence in the federal indictment against Park Jin Hyok</i>	13
<i>FIGURE 6: Fraudulent account lockout text messages are often more difficult to spot than email messages</i>	13
<i>FIGURE 7: A sense of urgency from upper management can be a strong motivator for employees to act</i>	14
<i>FIGURE 8: These types of lures are especially popular during the holiday season</i>	14
<i>FIGURE 9: Job search email submitted in the Park Jin Hyok federal indictment.</i>	15
<i>FIGURE 10: Email from the Park Jin Hyok federal indictment luring the recipient to open an attached resume (zip file)</i>	15
<i>FIGURE 11: Real estate scam wiring instructions—account number belongs to fraudsters</i>	16
<i>FIGURE 12: The login screen looks legitimate, but the URL in the address bar does not point to a valid Google domain</i>	16
<i>FIGURE 13: Fake link in an email message presents this legitimate-looking bank login screen</i>	17
<i>FIGURE 14: The top 10 organizations that phishers impersonated September 1–October 31, 2018 (Source: Webroot)</i>	18
<i>FIGURE 15: Top 10 targets by industry, September 1 – October 31, 2018 (Source: Webroot)</i>	18
<i>FIGURE 16: Fake login screens for familiar, commonly used apps often trip up users (Source: Webroot)</i>	19
<i>FIGURE 17: Industry breakdown of the top 20 growing targets from September 2018 to October 2018 (Source: Webroot)</i>	20
<i>FIGURE 18: Top 20 growing targets and growth rate from September 2018 to October 2018 (Source: Webroot)</i>	20
<i>FIGURE 19: Malware by type blocked by F5's Security Operations Center</i>	21
<i>FIGURE 20: Counterfeit cards for sale</i>	23
<i>FIGURE 21: Credit cards and lifetime accounts (e.g., Spotify, Netflix, DirectTV) for sale on the darknet</i>	23
<i>FIGURE 22: An ad for selling stolen Starbucks card numbers</i>	24
<i>FIGURE 23: Average estimated cost of different breach types in millions of dollars</i>	25
<i>FIGURE 24: F5 phishing email with malicious link in the attached PDF requesting users log in with their F5 credentials</i>	27
<i>FIGURE 25: Example of a fake Adobe login screen requiring the user to supply credentials before opening the PDF file</i>	28
<i>FIGURE 26: Fake PayPal website created by a scammer and reached via a malicious link in an email message</i>	29
<i>FIGURE 27: Methods for distinguishing bots from humans</i>	31
<i>FIGURE 28: An example of a security alert sent to F5 employees from the Security Awareness team</i>	34

Executive Summary

In November 2017, F5 Labs published an introductory report entitled [*Phishing: The Secret of its Success and What You Can Do to Stop It*](#). A year later, it should come as no surprise to security professionals that phishing continues to be a top attack vector and, in many cases, is the tried-and-true, go-to initial attack vector in multi-vector attacks. Phishing attacks leading to breaches have been steadily rising for the past two years that F5 Labs has been monitoring breaches. In 2018, we expect phishing attacks to surpass web application attacks to become the number one attack vector leading to a breach.

Phishing attacks leading to breaches have been steadily rising for the past two years that F5 Labs has been monitoring breaches.

50%

JUMP IN PHISHING AND FRAUD FROM OCTOBER-JANUARY

In this report, we look more specifically at the problem of phishing and fraud during the so-called “holiday season,” beginning in October and continuing through January. Based on data from a variety of sources, including F5’s Security Operations Center for Websafe and our data partner Webroot, we look at phishing and fraud trends over a year, the top impersonated companies in phishing attacks by name and industry, the growth rate in phishing attacks, and the fastest growing targets. We looked at how phishing works, the most common and successful phishing lures, what happens when a phishing attack is successful, and what types of malware can be installed.

We analyzed breaches that started with phishing attacks to provide context to the impact of phishing. We also analyzed what percentage of phishing domains leverage encryption to appear more legitimately like the sites they are impersonating, and malware sites that leverage encryption to hide from typical intrusion detection devices. As with most threats, phishing woes can be solved with people, process, and technology, so we close out the report with an extensive list of recommendations to defend your business against phishing and fraud.

KEY HIGHLIGHTS:

- Phishing and fraud season ramps up in October, with incidents jumping over 50% from the annual average, so be on the lookout now, and start warning your employees to do the same. Training employees to recognize phishing attempts can reduce their click-through rate on malicious emails, links, and attachments from 33% to 13%.
- Common phishing lures are known and should therefore be a key focus of your security awareness training.

71%

OF PHISHING IMPERSONATES
JUST 10 ORGANIZATIONS

- Seventy-one percent of phishing attacks seen from September 1 through October 31, 2018 focused on impersonating 10 top-name organizations, which is good news for your security awareness training programs as you now have a defined list to share with employees. The bad news is, the organizations happen to be the most widely used email, technology, and social media platforms on the Internet, so phishing targets everyone.
- With the cloning of legitimate emails from well-known companies, the quality of phishing emails is improving, and fooling more unsuspecting victims.
- Financial organizations are the fastest growing phishing targets heading into the holiday phishing season, but we expect to see a rise in ecommerce and shipping starting now.
- Attackers disguise the malware installed during phishing attacks from traditional traffic inspection devices by phoning home to encrypted sites. Sixty-eight percent of the malware sites active in September and October leverage encryption certificates.
- Reducing the amount of phishing emails that creep into employee mailboxes is key, but you also need to accept the fact that employees will fall victim to a phishing attack. Prepare your organization with containment controls that include web filtering, anti-virus software, and multi-factor authentication.

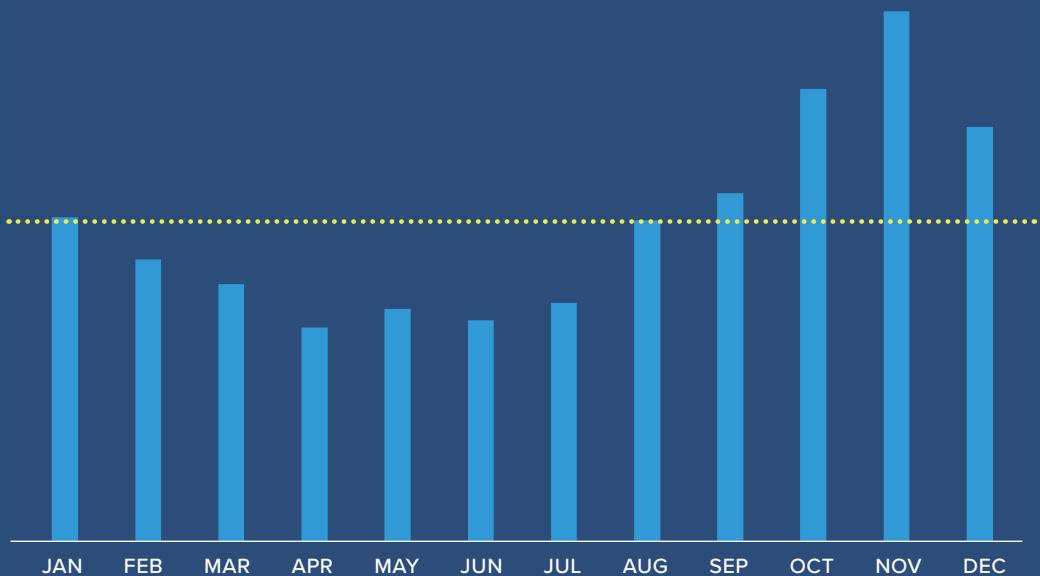


Introduction

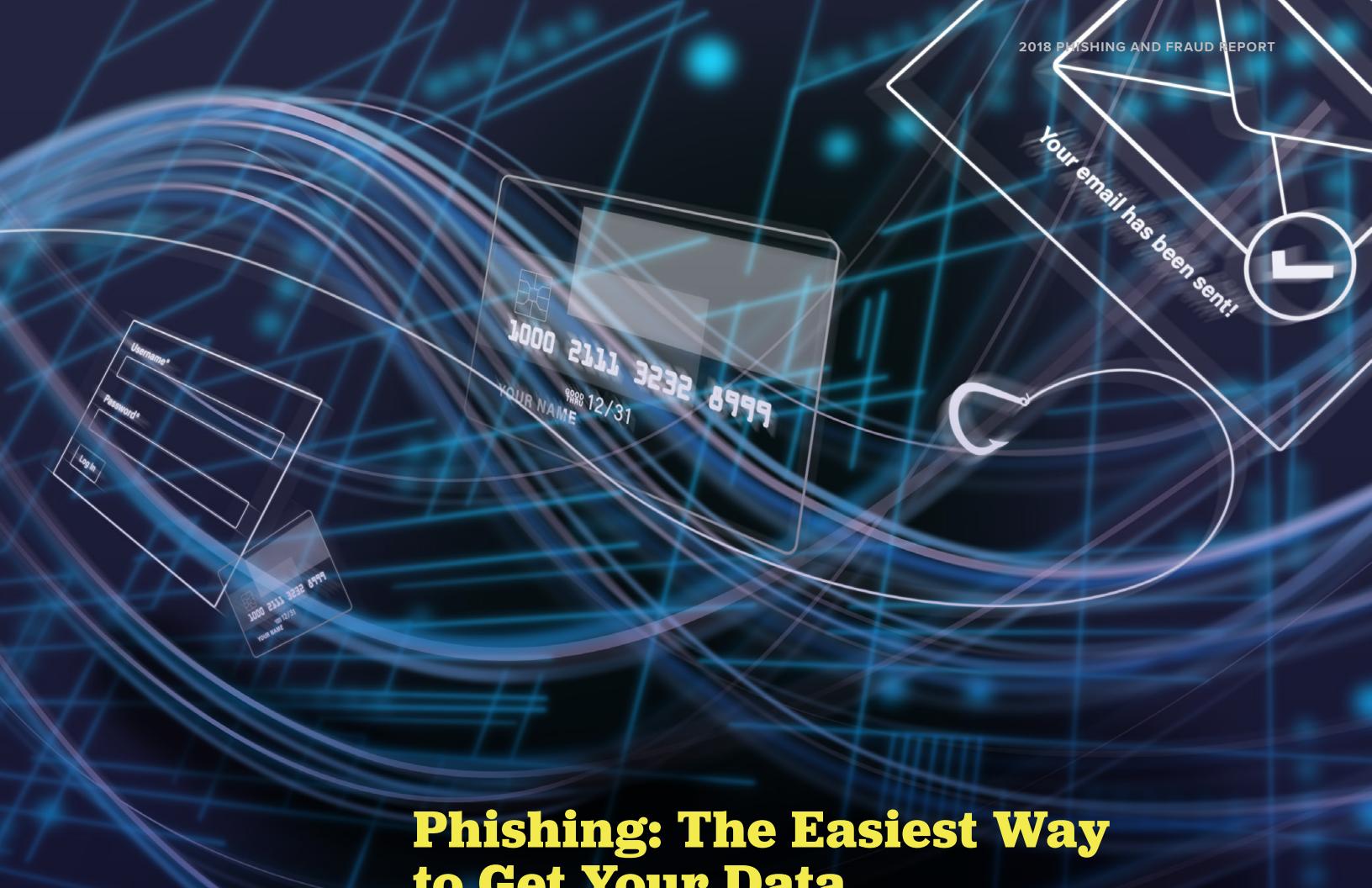
Fall isn't just about gingerbread lattes and holiday feasts. It's also peak season for phishing, when scammers use email, text messages, and fake websites to trick people into giving up their personal information. It's "prime crime time" when phishers and fraudsters creep out of their holes to take advantage of people when they're distracted: businesses are wrapping up end-of-year activities, key staff members are on vacation, and record numbers of online holiday shoppers are searching for the best deals, spending more money than they can afford, looking for last-minute credit, and feeling generous when charities come calling.

Data from the F5 Security Operations Center (SOC) for Websafe, which tracks and shuts down phishing and fraudulent websites for customers, shows that fraud incidents in October, November, and December jump over 50% from the annual average.

FIGURE 1: F5 Security Operations Center data shows fraud incidents jump significantly in October, November, and December



Data from the Retail Cyber Intelligence Sharing Center (R-CISC) echoes the F5 SOC findings and shows that dramatic increases in shopping activity actually continue into January, making retailers a likely target of attackers.¹ In a 2018 survey of R-CISC members, respondents expressed their concern, identifying phishing, credential compromise, and account takeover (ATO) among their top threats and challenges.²



Phishing: The Easiest Way to Get Your Data

Holiday season or not, phishing continues to be a major attack vector for one simple reason: *access is everything*—and phishing attacks give attackers access. Login credentials, account numbers, social security numbers, email addresses, phone numbers and credit card numbers are all pure gold to scammers—they'll steal any information that will give them access to accounts.

In F5 Labs' report [Lessons Learned from a Decade of Data Breaches](#), phishing was found to be the root cause in 48% of breach cases we investigated. Not only is phishing the number one attack vector, it's considered the most successful because it nets the greatest number of stolen records and therefore has the highest potential impact.

F5 Labs analysis of breach reports to state attorneys general from April to August 2018 revealed that in 86% of cases where personally identifiable information (PII) was compromised, the initial attack vector was phishing—that is, access to confidential data was obtained by an unauthorized person. In 8% of the reported cases, US employees' W-2 (wage and tax statement) information was requested in phishing emails that appeared to come from a legitimate email address. And in 5% of cases, customers were phished using email contacts stolen from a previously unidentified breach, which had compromised the PII of those customers.

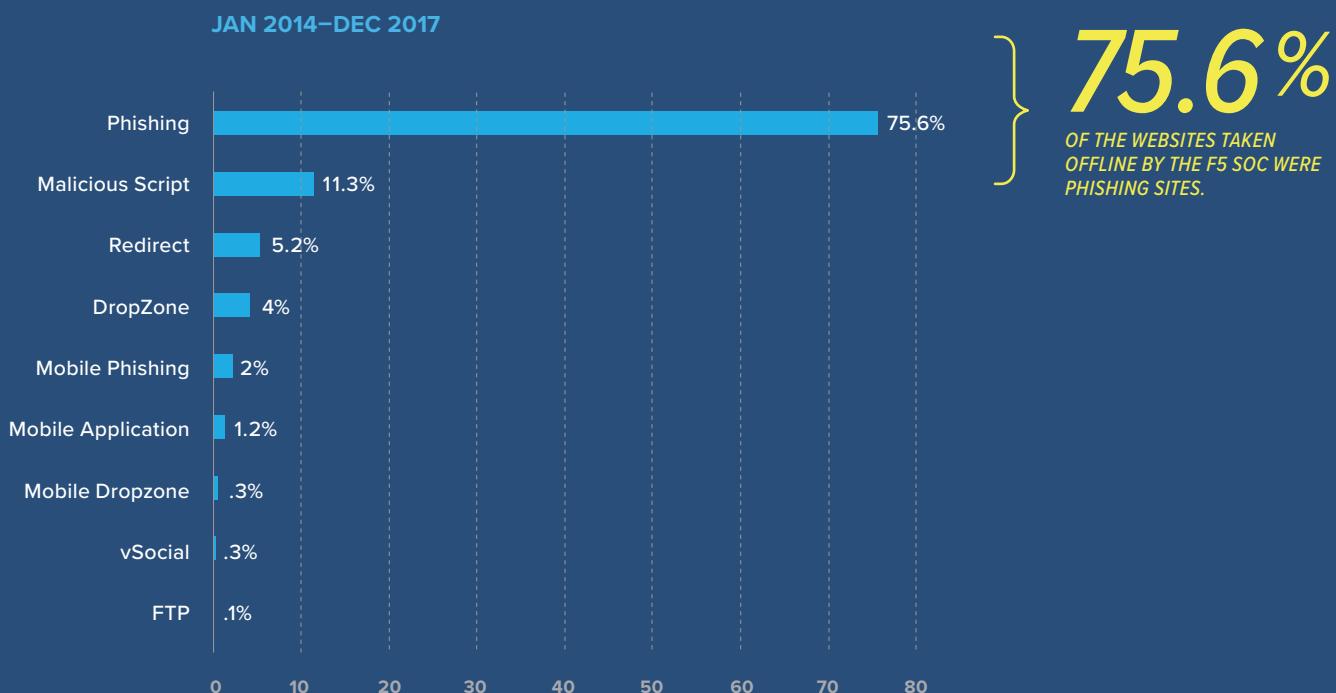


FIGURE 2: The majority of fraud sites shut down by F5's Security Operations Center are phishing sites

Figure 2 summarizes the types of websites the F5 SOC for Websafe has taken offline from January 2014 to the end of 2017. The overwhelming majority are phishing sites (75.6%), followed by malicious scripts (11.3%) and URL redirects (5.2%), which are also used in conjunction with phishing operations. Mobile phishing (2%) makes an appearance as a trending new problem, as well.

Some of the worst cyberattacks we read about in the news (and are affected by personally) are actually multi-layer attacks that use phishing as their initial attack vector. The federal indictment filed against North Korean national Park Jin Hyok bears this out. The US indictment, made public in September 2018, names Park as a co-conspirator in the 2017 WannaCry ransomware attack, the theft of \$81 million from a Bangladesh bank, and the 2014 attack on Sony Pictures Entertainment.

According to the indictment, Park's methods in these attacks include spear-phishing, destructive malware, exfiltration of data, theft of funds from bank accounts, ransomware extortion, and propagation of worm viruses to create botnets. In the indictment, FBI Special Agent Nathan P. Shields states, "...such spear-phishing emails that are the product of reconnaissance are often highly targeted, reflect the known affiliations or interests of the intended victims, and are crafted—with the use of appropriate formatting, imagery, and nomenclature—to mimic legitimate emails that the recipient might expect to receive."³

How Phishing Works

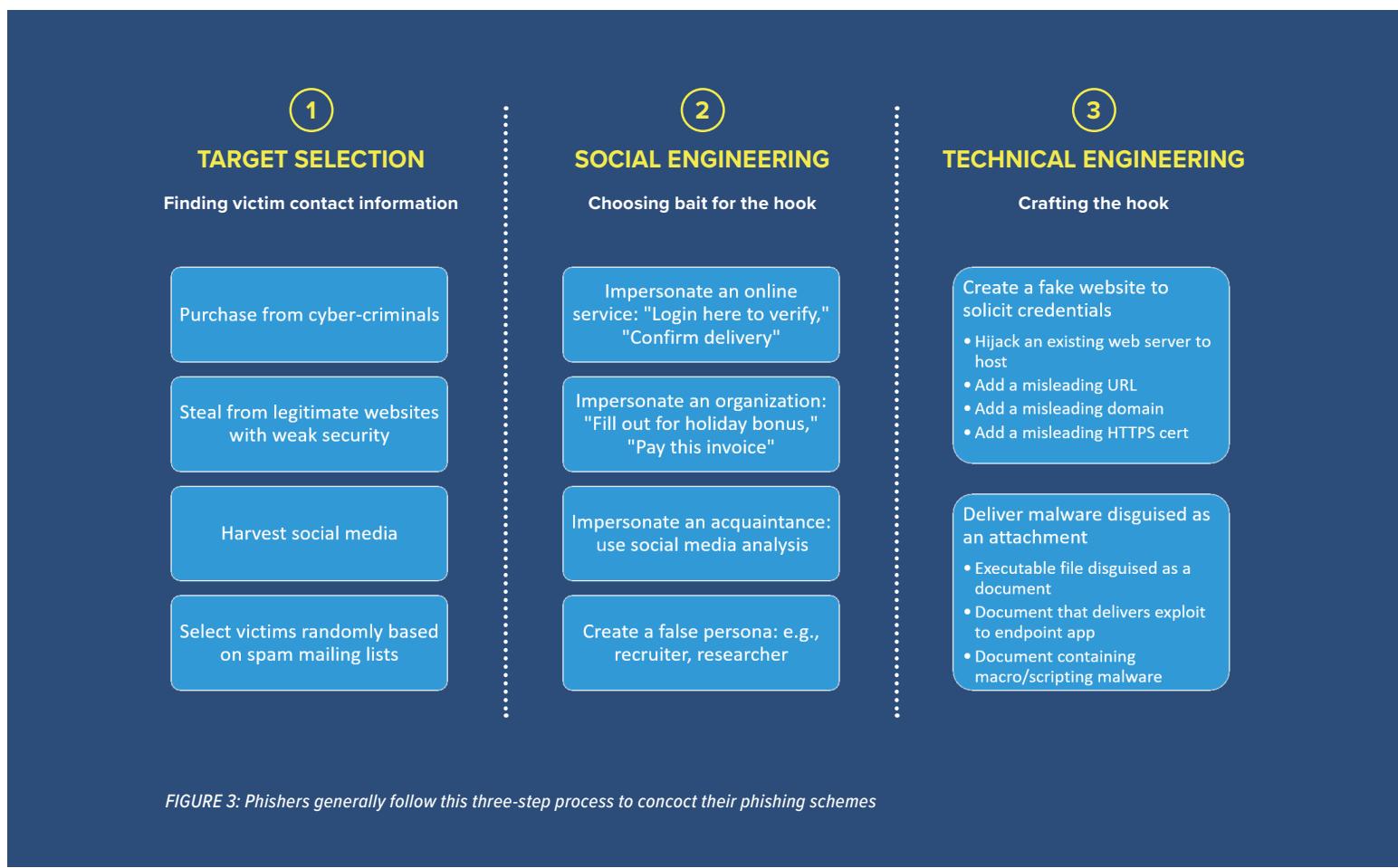
The technologies and methods of phishing scams are well-known and have not changed much over the years: a psychological hook is used to lure victims into trusting imposter web forms and applications. The general strategy of a phisher involves three distinct operations:

1. Target selection. Finding suitable victims, notably, their email addresses and background information to find a psychological hot button that will lure them.

2. Social engineering. Baiting the hook with a suitable lure that would entice a victim to bite into the technical hook set to steal their credentials or plant malware. In the case of spear-phishing, this lure is customized to the targeted victim. At the end of the year, phishers will take advantage of fiscal year-end and holiday events as part of their masquerade.

3. Technical engineering. Devising the method to hack the victim, which can include building fake websites, crafting malware, and hiding the attack from security scanners.

Target selection is something F5 Labs explored in depth in our report, [Phishing: The Secret of its Success](#). Because people voluntarily provide so much useful information about themselves online—and because so much information is for sale as a result of large-scale data breaches—it's getting easier for scammers to specialize their phishing campaigns, making them more effective.





Impersonation is a Key Tactic

Early phishing emails were much easier to spot with their poor-quality images and obvious spelling and grammatical errors. But today's phishers are upping their game with emails that look legitimate and appear to come from real companies and organizations.

One way they're accomplishing this is by cloning real emails. Quoting again from the federal indictment against Park Jin Hyok: "...the subjects of this investigation copied legitimate emails nearly in their entirety when creating spear-phishing emails but have replaced the hyperlinks in the legitimate email with hyperlinks that would re-direct potential victims to infrastructure under the subjects' control."

If scammers can impersonate an organization, why not real people, too? Park also used this tactic in his phishing schemes. "...the subjects created email accounts in the names of recruiters or high-profile personnel at one company (such as a U.S. defense contractor), and then used the accounts to send recruitment messages to employees of competitor companies"

Another tactic of scammers is to create websites for fake organizations with names so similar to real ones, they're enough to trip up users. Think about how many fake charitable websites have been created around helping wounded veterans, or fake insurance and healthcare companies whose names sound like real companies—or sound exactly the same but are spelled differently. Phishers even go out of their way to install encryption certificates on these sites to appear more legitimate. Ninety-three percent of the phishing domains Webroot collected in September and October 2018 offered a secure ([https](https://)) version of the site.

93%

OF PHISHING DOMAINS
OFFERED A SECURE (HTTPS)
VERSION OF THE SITE



877.967.6777 1878.5060

password

Common Phishing Lures

The most successful phishing lures play on people's emotions (greed, concern, urgency, fear, others) to get them to open an email and click on something.

Here are some of the most common lures:

BILLS OR INVOICES

Money always gets peoples' attention. This "Due Invoice" phishing email purportedly was sent from an F5 executive to a vendor, urging them to respond to the email message about their overdue account. Note the awkward phrasing and the excuses for being unavailable.

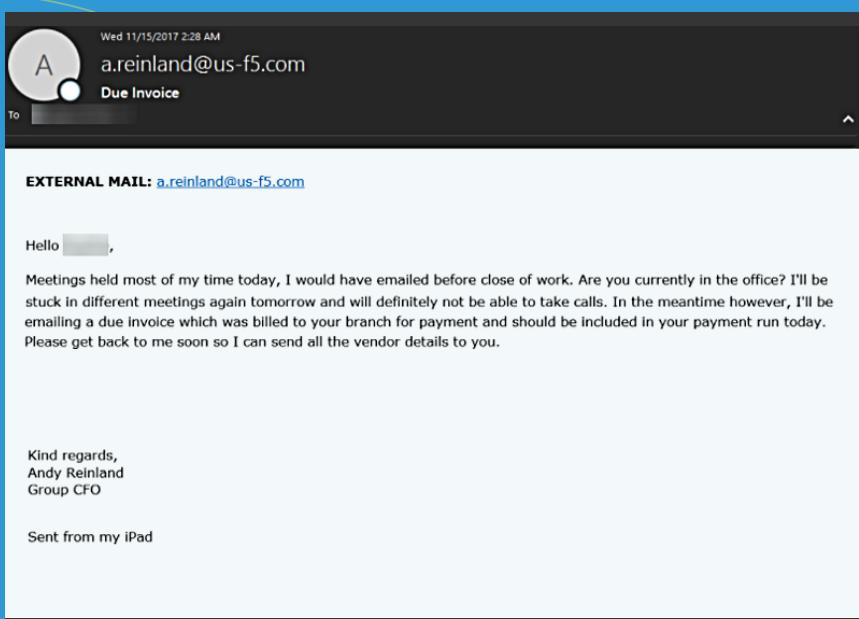


FIGURE 4: Phishing emails regarding bills or invoices often contain malicious links and documents

ACCOUNT LOCKOUT

A fake alert appearing to come from a familiar account (like Facebook, as shown in this example) telling the user they've been locked out of their account until they "click here" to provide additional information. (Note the fake "From" email address in the Facebook example is the tip-off that this is a scam.) Similar fake emails purporting to be from Google have been sent to recipients alerting them that they have been locked out of their accounts because "Malicious activities are detected."

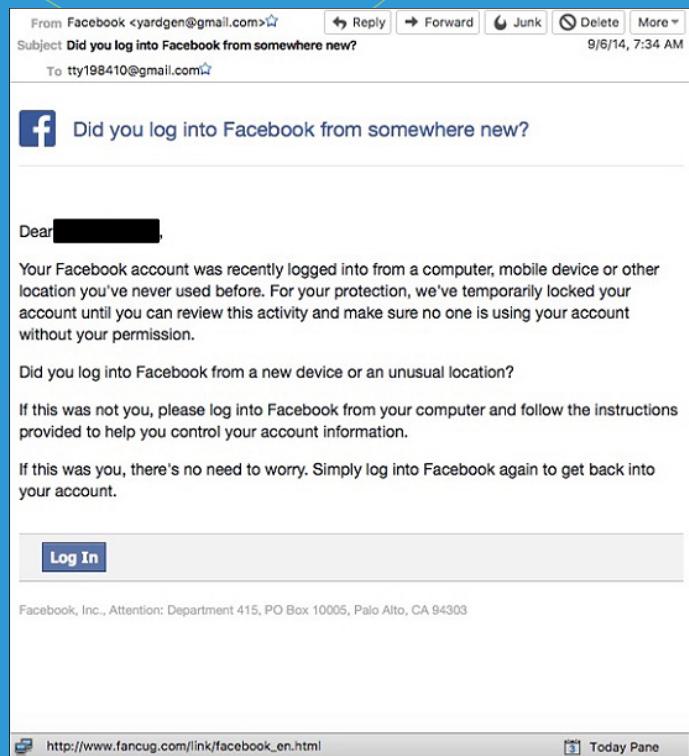


FIGURE 5: Fake Facebook phishing email—evidence in the federal indictment against Park Jin Hyok

TEXT MESSAGES

Text messages like this one appearing to come from Apple are often much more difficult to identify as a scam because they are generally brief and have fewer graphical cues (like a familiar logo) to tip off the user. The clue here is the awkward wording.

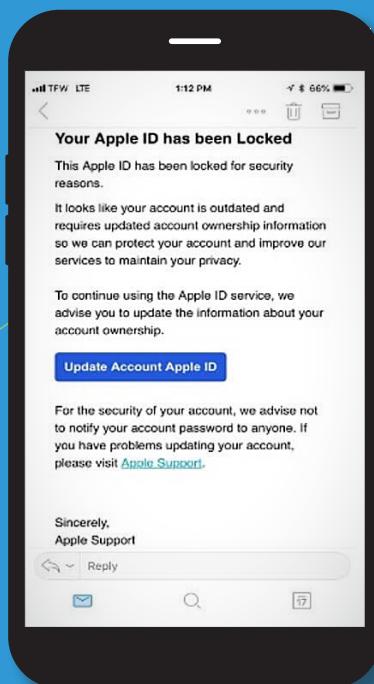


FIGURE 6: Fraudulent account lockout text messages are often more difficult to spot than email messages

AUTHORITY FIGURES/ EXECUTIVE STAFF

Employees often respond quickly to email requests from upper management or executives. This phishing email with the “Urgent” subject line was supposedly sent by F5’s CEO to an employee. (Note the “EXTERNAL EMAIL” warning label, discussed later in the Technological Defenses section. (This should be an internal email and would never be marked as External.)

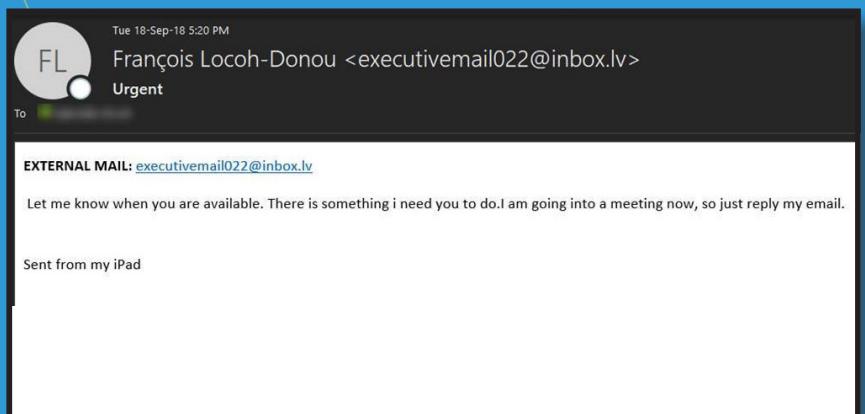


FIGURE 7: A sense of urgency from upper management can be a strong motivator for employees to act

ORDER OR DELIVERY INFORMATION/CONFIRMATION

Emails containing links where the recipient can check the status of an order or confirm receipt of a package (often the recipient isn’t even a customer).

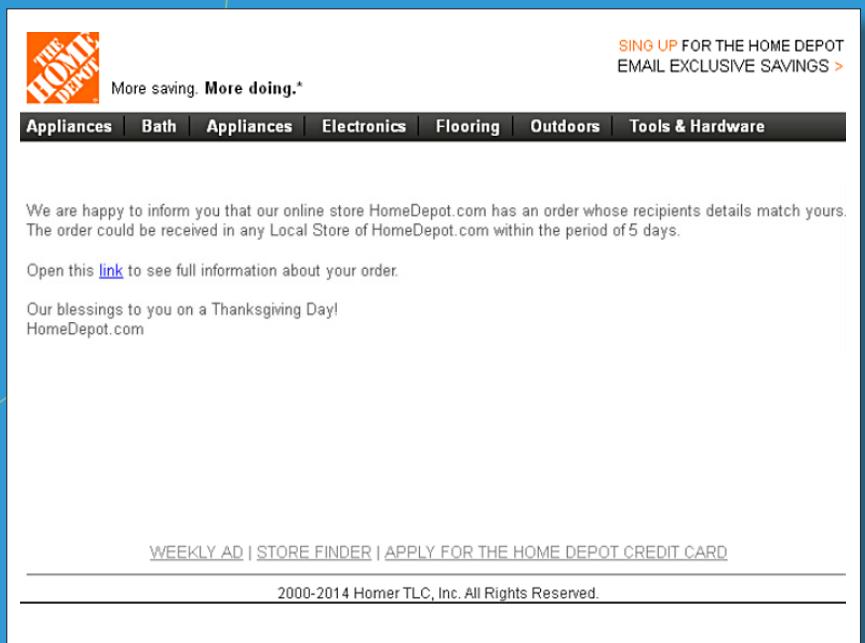


FIGURE 8: These types of lures are especially popular during the holiday season

RECRUITING AND JOB SEARCH

Email from a recruiter or high-profile individual of a competitor urging the recipient to open an attachment to view a resume or job description.

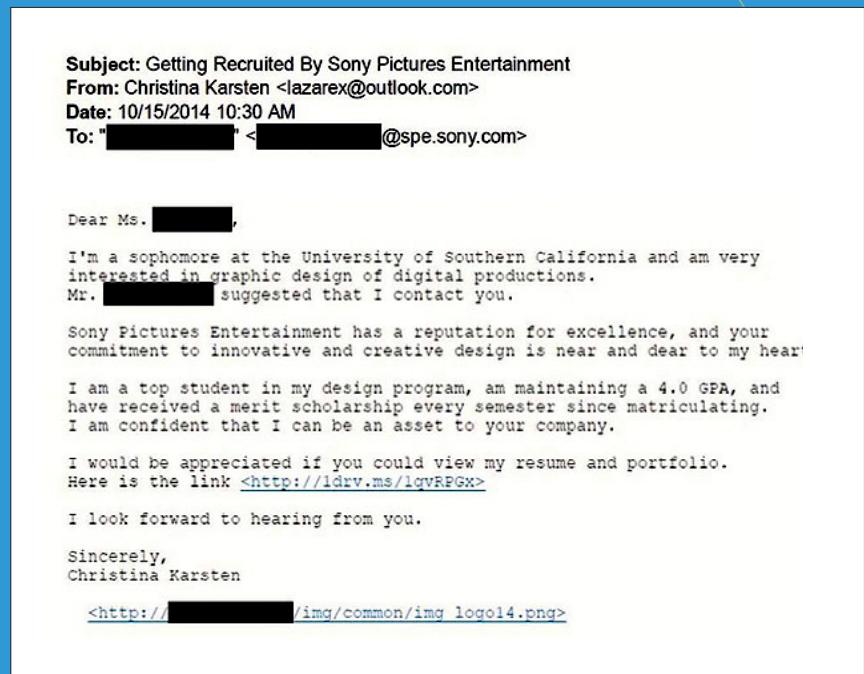


FIGURE 9: Job search email submitted in the Park Jin Hyok federal indictment.

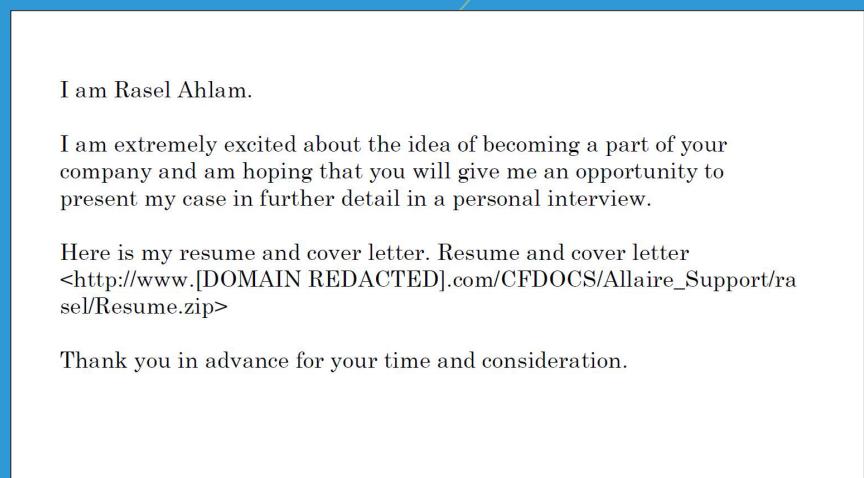


FIGURE 10: Email from the Park Jin Hyok federal indictment luring the recipient to open an attached resume (zip file)

REAL ESTATE/WIRE TRANSFER SCAMS

Emails that appear to come from a home buyer's real estate agent on or near their scheduled closing date of a property. The email contains an attachment giving the buyer new (different) money wiring instructions that point to the scammer's bank account.

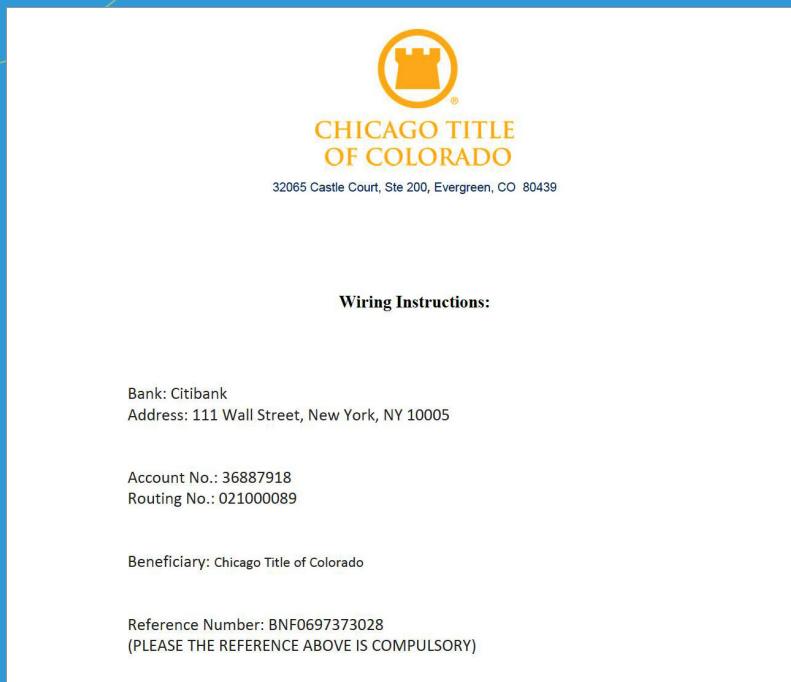


FIGURE 11: Real estate scam wiring instructions—account number belongs to fraudsters

“TRUSTED PARTY” LURES

These emails play on the victim's trust and familiarity with the sender. They appear to come from a friend or co-worker (who often was previously phished and compromised) and contain an attachment to review or a link to a website. A particularly convincing version of this used an email subject line of “Documents” and contained a URL that appears to go to a Google URL (but not Google Docs). Instead, it points to the scammer's site, which was hosted on Google, making it look legitimate.

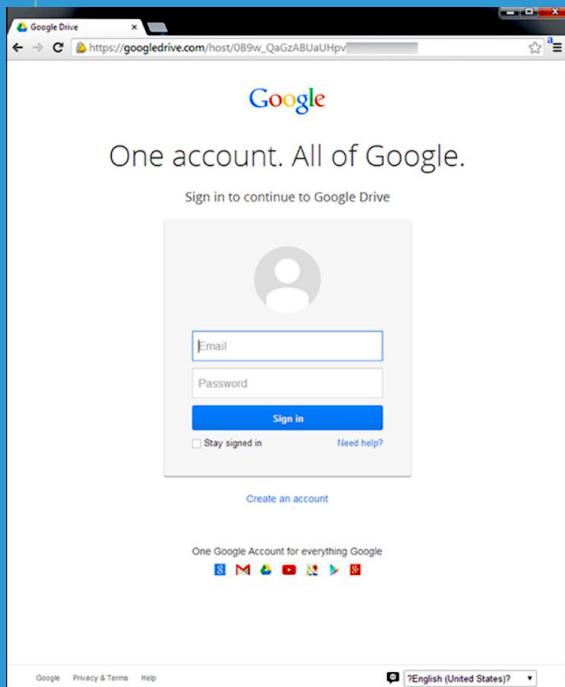


FIGURE 12: The login screen looks legitimate, but the URL in the address bar does not point to a valid Google domain

BANK ACCOUNT NOTIFICATION

Email appearing to come from the victim's bank saying "click here to login and get your bank statement."

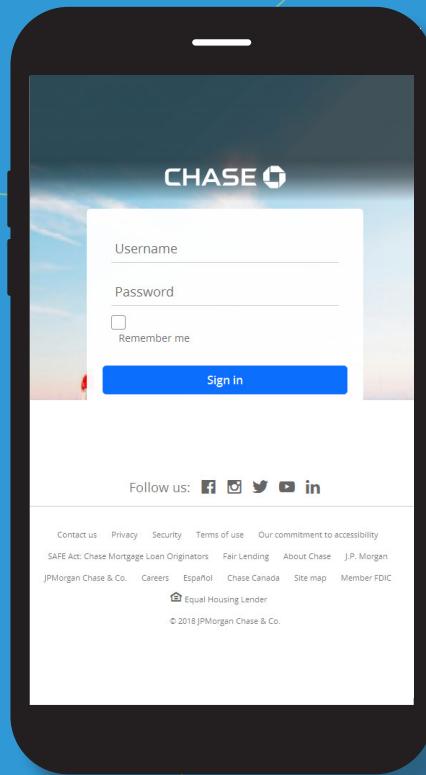


FIGURE 13: Fake link in an email message presents this legitimate-looking bank login screen

Other common phishing lures include:

DONATION REQUESTS

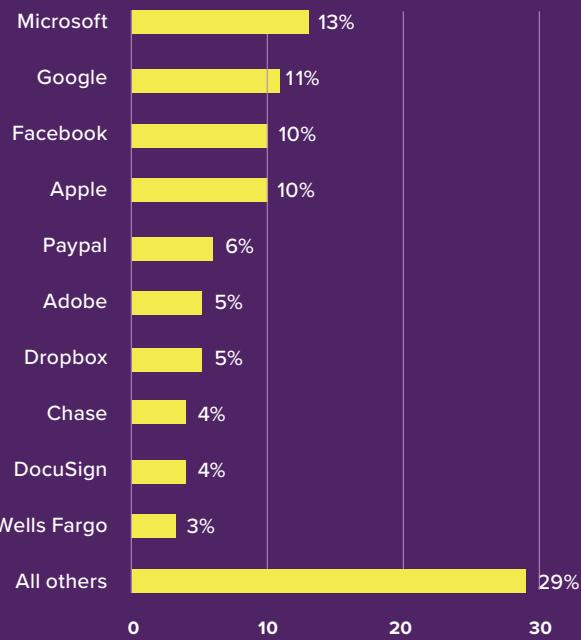
Email requests from well-known charities soliciting donations. These are especially prevalent during holiday season.

LEGAL SCARES

Email or voicemail warnings from the IRS, a collection agency, or government agencies saying you owe money and threatening legal action.

REFUND OR PRIZE NOTIFICATIONS

Often from the IRS or other organizations that supposedly owe you a refund or have a prize for you to claim.



SEPTEMBER–OCTOBER

FIGURE 14: The top 10 organizations that phishers impersonated from September 1–October 31, 2018 (Source: Webroot)

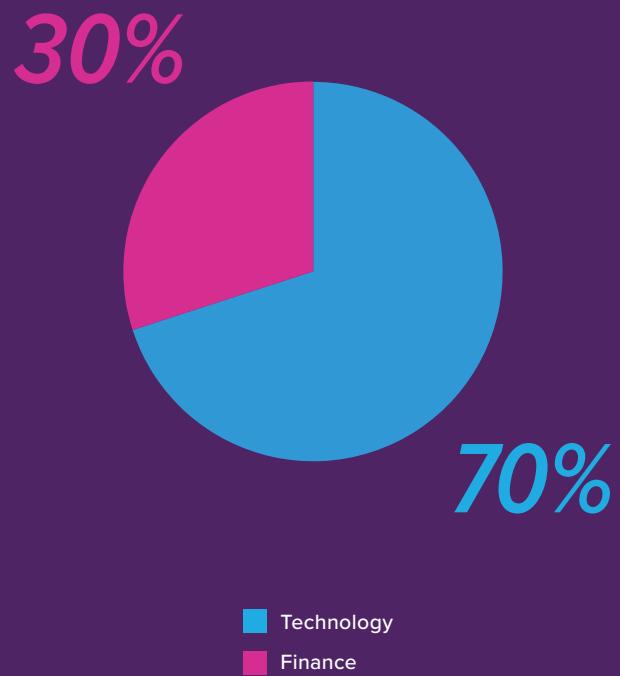


FIGURE 15: Top 10 targets by industry, from September 1–October 31, 2018 (Source: Webroot)

Top 10 Impersonated Organizations

Although phishing targets vary based on the scam the attackers are currently running, most of their efforts (over 71%) from September 1 through October 31, 2018 focused on impersonating 10 organizations. These organizations, collected by our partner Webroot, were predominantly in the technology industry and included software and social media companies; email and document sharing providers; and financial organizations, including banks and one payment processor.

Phishers impersonated some of the most popular Internet services in the world. By spoofing these most commonly used services in combination with one of the familiar lures (described in the previous section), phishers increase the chances that an unsuspecting victim will trigger their malicious link or document. Targeted technology organizations included Microsoft, Google, Facebook, Apple, Adobe, Dropbox, and DocuSign. Phishers pretended to impersonate them 58% of the time throughout September and October.

When looking at targets by industry, technology organizations represented 7 of the top 10 targets, followed by financial organizations.

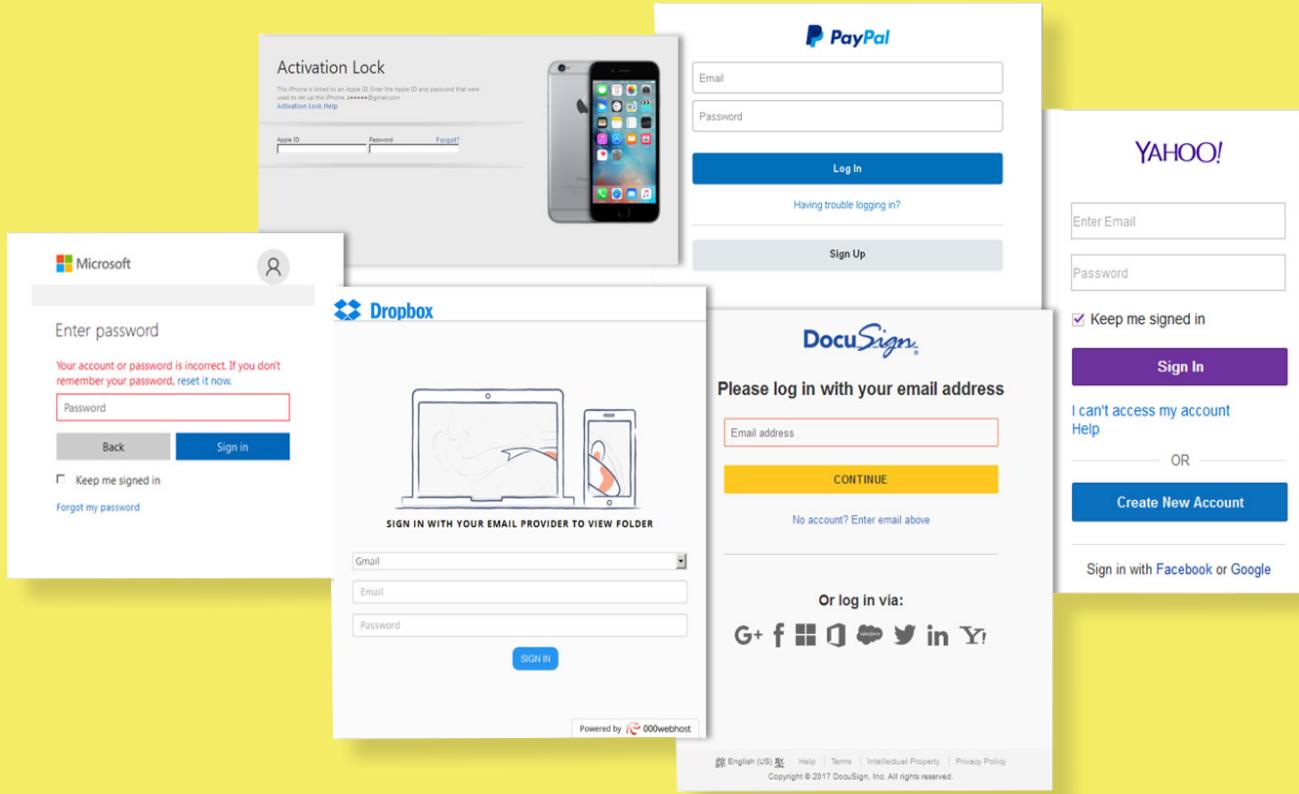


FIGURE 16: Fake login screens for familiar, commonly used apps often trip up users

Sometimes the goal is to capture a user's email credentials, which can be a gateway to other critical services like online banking logins. Other services, such as DocuSign, Adobe, and Dropbox, are used to send documents fraud victims are likely to open that are often embedded with malware or offer an avenue for the victim to submit their financial information (see Figure 16).

When organizations are conducting security awareness training, employees should be warned to stay vigilant and wary when it comes to email that appears to come from one of the providers shown above.

Notably missing are shipping and ecommerce targets, which we expect to see rise as the holiday shopping season ramps up.

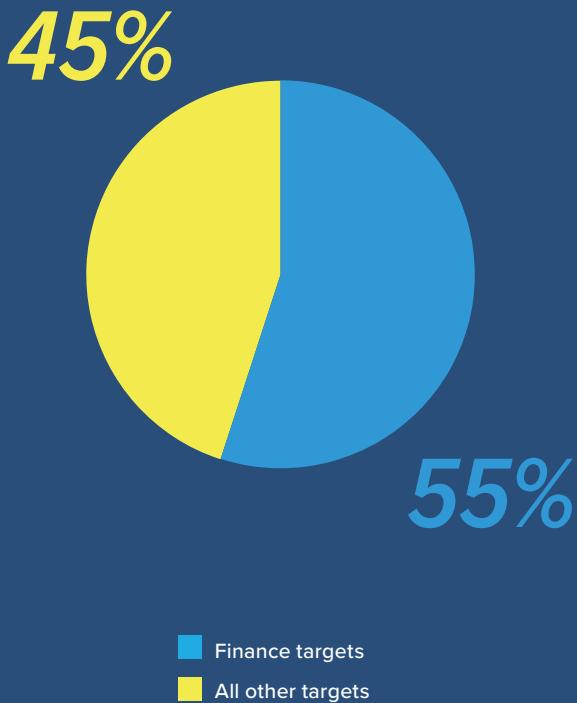


FIGURE 17: Industry breakdown of the top 20 growing targets from September 2018 to October 2018 (Source: Webroot)

Target	Growth	Industry
STRIPE	1,267%	PMT PROCESSOR
WELLS FARGO	924%	BANK
BNP PARIBAS	800%	BANK
MBANK	800%	BANK
SMILES	700%	TRAVEL
COMCAST BUSINESS SERVICES	674%	TELECOM
BANKINTER	500%	BANK
NEDBANK	500%	BANK
BAWAG	462%	BANK
RIA	400%	PMT PROCESSOR
CAPITAL ONE	333%	BANK
RABOBANK	329%	BANK
HSBC	320%	BANK
GOOGLE	318%	TECH
ADOBE	305%	TECH
LINKEDIN	300%	SOCIAL
USAA	275%	BANK
BITCOIN	243%	CRYPTOCURRENCY
TARGET	206%	ECOMMERCE
BCP	204%	BANK

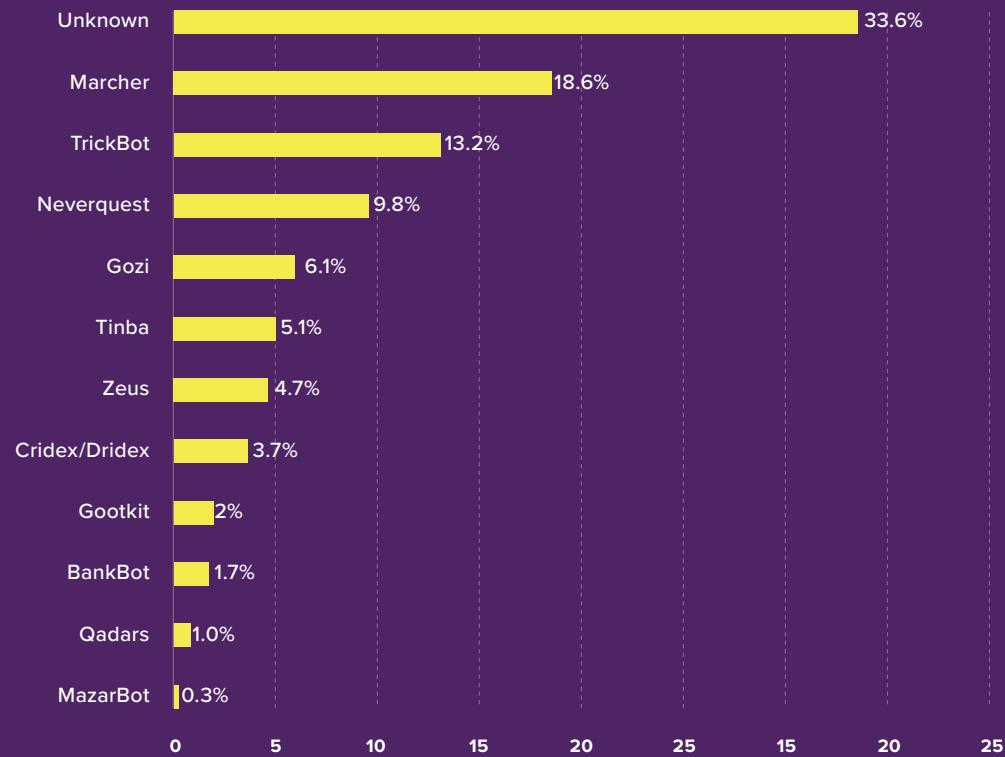
FIGURE 18: Top 20 growing targets and growth rate from September 2018 to October 2018 (Source: Webroot)

To see emerging threat trends, Webroot looked at the top 20 growing targets. While a month-over-month comparison is not a strong basis to confirm a longer-term trend, high percentage growth is an indication of attacker interest in particular target customers or industries. From September 1 to October 31, 2018, 13 of the top 20 fastest growing targets were financial organizations. Stripe, a popular payment processor, topped the list with a 1,267% growth rate.

From September 1 to October 31, 2018, 13 of the top 20 fastest growing targets were financial organizations.

Banks accounted for 55% of the top 20 growing targets and are a good example of how widespread phishing is across the globe. Five of the banks service customers primarily in Europe, and three (including one payment processor) service customers primarily in Latin America.

FIGURE 19: Malware by type blocked by F5's Security Operations Center



Malware Attacks that Target Credentials

Malware can be designed to do many different things, but eventually it must find its way onto a victim's computer in order to be effective. One of the most common ways is through an initial phishing campaign.

Some of the most successful malware programs that collect login credentials actually started out as banking malware. [Trickbot](#), along with Zeus, Dyre, Neverquest, Gozi, GozNym, Dridex, and Gootkit, are all banking trojans known to have spread initially through phishing campaigns. Many of these banking trojans have been around for years, and the authors continue to refine and reinvent them, adding new functionality. Some have also expanded their targets well beyond banks to include popular retailers like Best Buy, Victoria's Secret, Macy's and others, as was the case with [Ramnit](#).

In 2018, [Panda](#) malware, a spinoff of the Zeus banking trojan, expanded its targets to include cryptocurrency exchanges and social media sites. So, while the ultimate goal of most of these banking trojans is to steal money, most have the ability to steal credentials, too.

How Malware Steals Credentials

There's no end to the creativity of malware authors and the [innovative changes](#) they'll make with every new malware campaign, but we've already seen that stealing credentials is a key step along the way, regardless of their ultimate objective. Here are some of the techniques used by malware to steal credentials:

- Changing browser proxy settings to redirect traffic through the malware running locally on the victim's client. Then all web traffic can be inspected and rewritten before TLS encryption is applied.
- [Screen shots, clipboard pastes, and keylogging](#) are techniques used by malware to capture login credentials and other sensitive information typed in by the user on their computer or mobile device. They're typically downloaded to a user's system, just like any other type of malware.
- Malware like the banking trojan [BackSwap](#) injects JavaScript code into a targeted banking web page that creates fake input fields visible to the victim. These fake fields hide the real fields on the webpage, which are prepopulated with the fraudster's banking information, and it is these fields that are submitted when the victim executes a transaction.

How Scammers Use Stolen Access to Loot Apps

Depending on the type of data that's stolen—personally identifiable information (PII); financial, healthcare, or educational details; credit card information—scammers will carry out different types of crime. When they have login credentials—especially for bank accounts—they can quickly log in, take over the account, and then drain off all the cash. Sometimes they'll pivot and go after other targets. In other cases, say, with stolen credit card data, the thieves try to sell that data on the darknet. In turn, the buyer might do any of the following:

Create fake credit cards by loading card numbers onto card blanks (cashout services) and using them in ATMs to get cash, or online to make purchases.

FIGURE 20: Counterfeit cards for sale

Demand For Physical Plastic? by [BMDTeam](#) in Fraudnet2
 ↑ [-] [BMDTeam](#) [S] 1 point 18 hours ago
 I like the "just selling embossed cards" part. The only problem I can see there is that we would have no info emboss on the card as, well the customer wants to write their own information.
 As per prices, I was thinking something as \$40 for a base price and then:
 +\$10 for a classic / standard
 +\$15 for a premier / gold
 +\$20 for a business / platinum
 +\$25 for a world / purchasing
 Worth it from a buyers perspective?

FIGURE 21: Credit cards and lifetime accounts (e.g., Spotify, Netflix, DirectTV) for sale on the darknet

Buy services like Netflix, Spotify, DirectTV or online games for a fraction of the original cost.

		Recommended	Escrow / multisig / FE	Top vendors only
	100 € Paypal Account From EU		18.57 EUR	Dr.Whit3 (521 / -8)
	200\$ US Paypal Accounts Balance		20.43 EUR	Dr.Whit3 (521 / -8)
	NETFLIX.COM - [LIFETIME NETFLIX PREMIUM ACCOUNT]		9.28 EUR	Woody (253 / -4)
	FUD BTC STEALER SOURCE CODE + SPREADING GUIDES		9.28 EUR	passman (702 / -7)
	SPOTIFY.COM - [LIFETIME SPOTIFY PREMIUM ACCOUNT]		9.28 EUR	Woody (253 / -4)
	Private Hacking Service		27.85 EUR	passman (702 / -7)
	custom listing yss1		15.79 EUR	Dr.Whit3 (521 / -8)
	HOW TO CASHOUT PAYPAL VIDEO + 12 BONUS GUIDES		4.63 EUR	passman (702 / -7)
	DIRECTV.COM - [LIFETIME DIRECTV PREMIUM ACCOUNT]		9.28 EUR	Woody (253 / -4)

Verify card numbers are valid with a small transaction (\$1.00) on a music site to confirm there is available credit to drain.

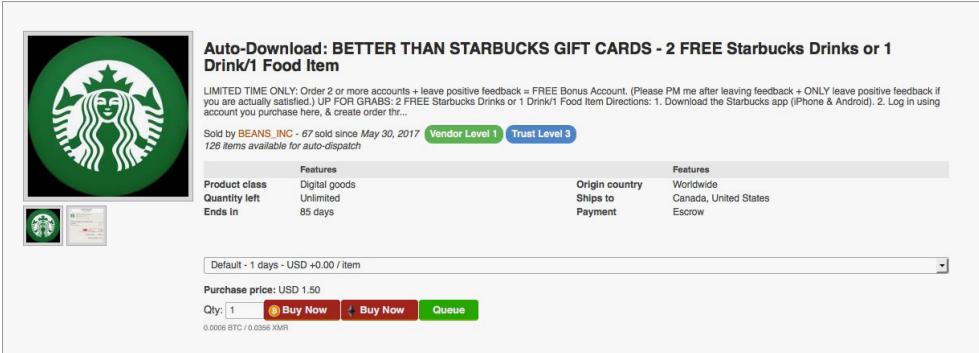
Hire or resell card numbers to “money mules” who are other scammers recruited to buy goods with the stolen card numbers and then reship those goods to other scammers for resale. This way, the stolen card number is laundered back to cash, albeit at a lesser value because of the resale.

Use the card numbers as part of another scheme, such as buying fake domains or web services to support other scams and hacking endeavors.

Buy compute services to mine cryptocurrency.

Sell stolen card numbers online.

FIGURE 22: An ad for selling stolen Starbucks card numbers



The screenshot shows an eBay listing for "BETTER THAN STARBUCKS GIFT CARDS - 2 FREE Starbucks Drinks or 1 Drink/1 Food Item". The listing is sold by BEANS, INC. with 67 sales since May 30, 2017, and has a Trust Level 3 rating. It indicates 126 items available for auto-dispatch. The product class is Digital goods, quantity is Unlimited, and it ends in 85 days. Features include Worldwide shipping to Canada and the United States via Payment and Escrow. The purchase price is USD 1.50 per item. The listing includes a "Buy Now" button and a "Queue" button. A note at the bottom states: "0.0006 BTC / 0.0396 XMR".

IN MILLIONS OF DOLLARS

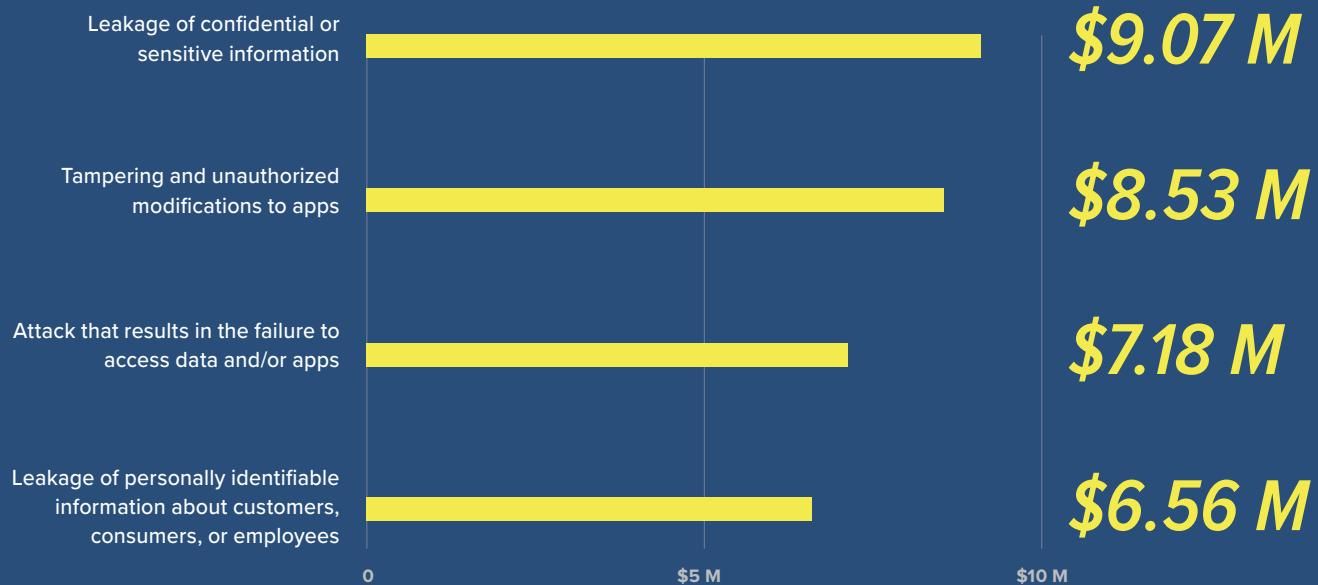


FIGURE 23: Average estimated cost of different breach types

Stolen Credentials Lead to Fraudulent Transactions

If you're one of the unlucky organizations who's had your data breached, it's going to be a PR nightmare no matter how you look at it, but that's only the beginning. You can also count on the applications you host being full of fraudulent transactions. Your customers whose credentials were stolen are going to be calling you when scammers start racking up fraudulent charges on their accounts. You'll be dealing with an onslaught of customer complaints, requests to reverse charges, fraud cleanup efforts, and trying to figure out how to repair your reputation without permanently losing customers. Based on survey data of 3,300 security professionals for F5 Labs' [2018 Application Protection Report](#), the average PII breach costs organizations \$6.5 million, and a breach that involves tampering with or unauthorized access to an application costs (on average) \$2 million more than a PII breach.

The insidious thing about data breaches is that they affect everyone—even companies who have not had their own data breached. Because so many people reuse passwords for multiple applications, accounts, and websites, even companies that haven't been breached will see an uptick in fraudulent activity due to credential stuffing attacks. Which is why it's in an organization's best interest to protect their own phished customers from themselves by buying bot-scrappers.

Defending Against Phishing and Fraud

Everyone—security pros and individuals alike—need to know how to defend against phishing and fraud. While it's in an individual's best interest to stay informed about the latest scams, they can never be expected to see or understand the warning signs the way security professionals do.

Teaching Users To Resist Phishing Lures

We can't overemphasize the importance of user awareness training—especially since phishing scams continue to get more sophisticated and aggressive. Many users don't take phishing seriously, thinking the odds of it happening to them are slim, or if it does happen, the impact might only be minor. Users need to be aware that phishing can be extremely harmful to them as individuals, enabling hackers to steal their money, make unauthorized purchases, assume their identity, open credit cards in their name, expose their PII on a broader scale, and sell it to other scammers. At the same time, it's equally dangerous to companies.

.....

Mike Levin, a guest author for F5 Labs and head of the Center for Information Security Awareness offers consumers advice on what to watch for:

First, it's critical for users to understand that *any email address can be faked or spoofed*. URL spoofing is the process of creating fake or forged URLs that are often used in phishing attacks. So, *never trust the display name in the email address*. Before you open the email, try hovering the mouse over the email address or links in the preview message to view the full information.

One of the riskiest “everyday” phishing scams happens when you receive an email that appears to be from someone you know such as a co-worker, family member, business colleague, or friend could be fake and contain malicious code. The criminal crafts a legitimate looking email from a familiar name or organization in hopes that the user will automatically open it. This is especially true for unexpected emails that contains links or attachments. When handling email:

- *Slow down and take your time deciding which messages to open.*
 - *Don't automatically open every email message. Ignore spam and delete it or mark it as junk mail.*
 - *When in doubt, research and contact the sender independently to verify an email is legitimate. Taking a few minutes to make a quick call or open a chat message to the sender can reduce your risk and help protect your data.*
 - *When in doubt, ask! Employees who give IT early warning of phishing attacks, successful or not, can make the difference between a near-miss and a major breach.*
 - *Be on the lookout every day for scams.*
-

33%
→ **13%**

*CLICK-THROUGH RATES
DROP FROM 33% TO 13%
WITH TRAINING*

As stated earlier, pay special attention to the top impersonated organizations. The best first line of defense for phishing is to create a culture of curiosity. Teach your users to ask questions first and click second.

Webroot testing has shown that the more security awareness training is conducted, the better employees are at spotting and avoiding risks. Companies that ran 1 to 5 training campaigns saw a 33% phishing click-through rate; those that ran 6 to 10 campaigns dropped the click-through rate to 28%; and those that ran 11 or more training campaigns reduced the rate to 13%. Additionally, phishing simulations and campaigns were found to be most effective when the content is current and relevant. This means that companies who don't conduct security awareness training can reasonably expect users to click on at least 1 in 3 phishing emails. Clearly, the training is worth the extra time, effort, and expense because any way you look at it, it's cheaper than dealing with a breach.

Things to Watch Out For

In addition to the tips above, users should be aware of the following:

PDF and Zip file attachments can contain malware and should only be opened when a user is expecting a trusted sender to attach them. With PDF files, some fraudsters attempt to capture victims' login credentials by putting up a fake login screen requiring the user to enter their Adobe username and password in order to open the file. Grammar and punctuation errors should be an obvious tip-off in the email shown in Figure 24.

FIGURE 24: F5 phishing email with malicious link in the attached PDF requesting users log in with their F5 credentials

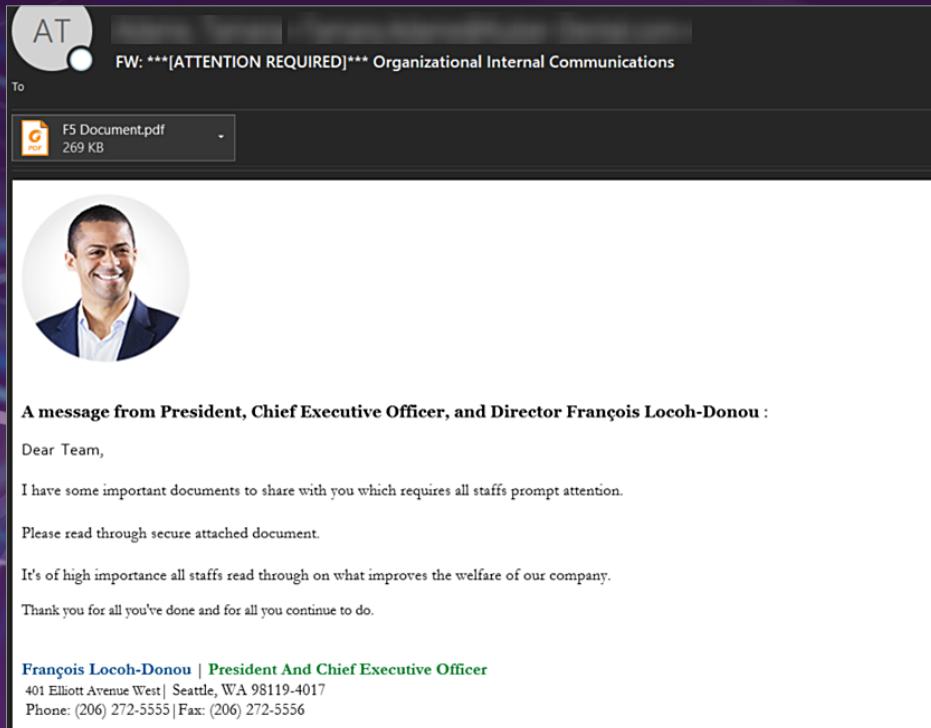
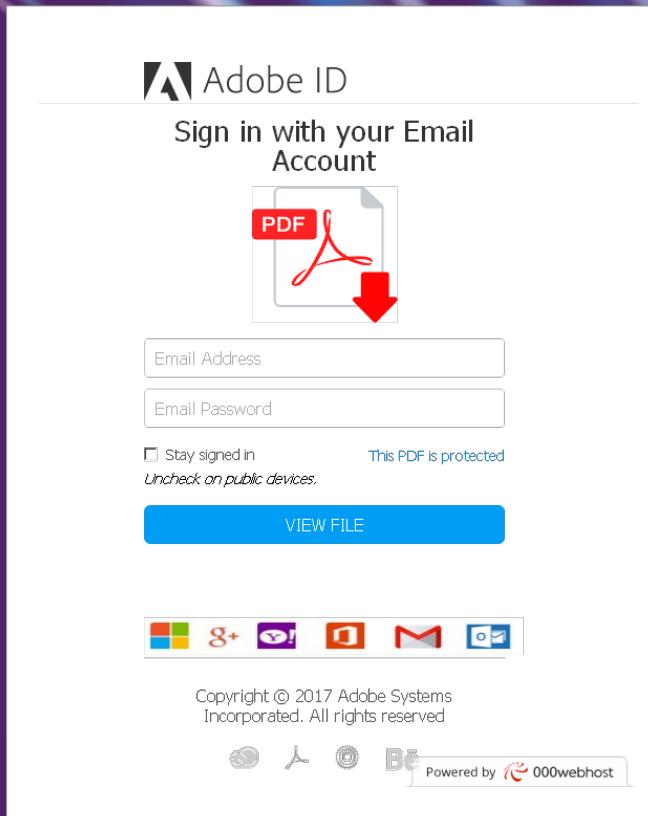


FIGURE 25: Example of a fake Adobe login screen requiring the user to supply credentials before opening the PDF file



Shortened URLs from services like bit.ly and others can be malicious, and hovering over the link won't reveal the actual URL. Services that expand URLs are available online, but it's best to check the safety of those services before using them. A better option is to open a new browser tab and search for the content or website that's referenced.

Certificate warnings are displayed by a user's browser when the security certificate of the website they've requested is invalid, not current, or has not been issued by a trusted certificate authority. Rather than ignore the warning, if a user thinks the site is legitimate, it's best to search for the site in a separate browser window.

Security alert emails marked "urgent" are an immediate red flag if the email also requests that the user provide login credentials, personal information, or click on a link or open an attachment. Users should try to verify the alert using some other means such as connecting directly to the sender's website or calling the help line.

Unexpected email from a friend, acquaintance, colleague, or business associate asking the user to provide sensitive information or to click on a link or open a file attachment. Users should try to confirm the request in some other way, such as sending a separate email to the sender's known, legitimate email address, sending a text or chat message, or calling a known, legitimate phone number for the sender.

Fake phishing websites can be extremely well crafted and look surprisingly legitimate, like the one shown in Figure 26, which was arrived at by clicking a malicious link in an email message. The URL, which has been blurred in this image, is not a legitimate PayPal domain. Users should not click on links in email, but if they do, they should make a habit of checking the URL in the address bar before providing any personal information such as login credentials or account information. Instead, they should try reaching the site directly in a separate browser session.

FIGURE 26: Fake PayPal website created by a scammer and reached via a malicious link in an email message



Technological Defenses

User awareness training is a great start and absolutely essential, but protecting your organization and users from phishing attempts requires technological measures, as well. Below are a few we recommend:

Email labeling. Clearly label all mail from external sources to prevent spoofing. A simple, specially formatted message like the following is sufficient to alert users to be on guard and proceed with caution.

CAUTION: This email originated from outside of the company. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Anti-virus (AV) software. Accept the fact that your users are going to get phished and rely on backup controls to prevent a phishing misstep from spreading malware throughout your environment. AV software is a critical tool to implement on every system a user has access to, most importantly, their desktops and laptops. In most cases, AV software will stop the malware installation attempt, as long as it's up to date, so set your AV policy to update at a minimum of daily.

Web Filtering. Plan for your users to get phished and have a web filtering solution in place to block access to phishing sites. When a user clicks on a link to a phishing site, their outbound traffic to that site will get blocked. Not only will this prevent a breach to your organization (providing the phishing site is known by your web filter provider), but it presents a valuable teaching opportunity by displaying an error message to the user saying: “Access to this phishing site has been blocked by your organization’s security policy...”

Traffic decryption and inspection (see *Inspect Encrypted Traffic for Malware* later in this report).

Single-Sign On (SSO). Deploying an SSO solution to reduce password fatigue is a good way to limit the impact of a successful phishing attack. The fewer credentials general users have to manage, the less likely they are to share them across multiple applications (the one-to-many impact of stolen credentials), create weak passwords they can remember, and store them insecurely. Given that password cracker databases [exceeded one trillion records in 2017](#) (before major breaches like Equifax and Facebook in 2018), enabling attackers to crack hashed credential databases in less than 6 hours, we all need to do our part to support the integrity of access control as a whole.

Multi-factor authentication should be required for all employees and all access, even email. Your users will get phished to steal their corporate credentials, and unfortunately, many of them use the same credentials across multiple sites. Even if an employee doesn’t get phished, you run the risk of organizational third-party services getting compromised, and their stolen credentials being used in a credential stuffing attack. Multi-factor authentication makes the second factor, such as a constantly changing code, very difficult to impersonate or steal.

Provide a means for employees to easily report suspected phishing, or instruct them to call the helpdesk or security team if they see a suspicious email.

Report phishing. Provide a means for employees to easily report suspected phishing. Some mail clients (like Microsoft Outlook) now have a phish alert button built in to notify IT of suspicious email. If your email client doesn’t have this feature, instruct all users to call the helpdesk or security team if they see a suspicious email. If the email turns out to be a phishing attempt, the security team can quickly delete it from mailboxes (so no one else is taken in by it) and warn all employees. Phishing attempts often come in waves, so when phishing happens, employees should look out for more.

Change email addresses. Consider changing the email addresses of commonly targeted employees if they are receiving an unusually high number of phishing attacks on a continual basis.

Use CAPTCHAs. Use challenge-response technologies like CAPTCHA to distinguish humans from bots. CAPTCHAs are effective, but users find them annoying, so use them in cases where it’s highly likely a script is coming from a bot.

Block bots (see *Bot Detection Responses* section later in this report).

Review access control. Review access rights of employees regularly, especially those with access to critical systems. Employees with access to critical systems should be prioritized for phishing training.

Look out for newly-registered domain names. Often phishing sites are newly registered domains, which is a telltale sign of fraudsters setting up fake websites that they use temporarily to pull off their schemes, and then abandon quickly. When we reviewed the list of active malware and phishing domains collected by Webroot in September, only 62% were still active a week later when we did whois lookups; 38% of them had disappeared.

Implement web fraud detection. Your clients are targeted with phishing attacks designed to infect their systems with fraud trojans. Implement a web fraud solution that detects clients infected with malware so they cannot log into your systems and thereby allow fraudulent transactions to occur.

Make use of honey tokens. Dummy user accounts and email address can be monitored to detect when attackers send out blanket phishing emails. If they have already infected a user's device, then a dummy account will let you know if the attacker is enumerating accounts in your domain.

How to Distinguish Between a Legitimate User and a Bot that Uses Stolen Credentials

Since phishing is often initiated by bots, and bots are active on your website every day, you need to know how to detect who's visiting your website—a bot or a human—in order to protect yourself. Some detection methods are more successful than others; in any case, you'll want to use a combination of methods.

Bot Detection Methods that are Prone to False Positives and Negatives

Several methods for detecting bots are prone to false positives (alerts generated in error) and false negatives (malicious events that generates no alert). Neither one is desirable—and arguably, false negatives are the worst-case scenario—but that doesn't mean you shouldn't consider the following:

- **IP geolocation and IP reputation.** Making security decisions based on these two pieces of information can eliminate a lot of bot traffic on your network, but it's getting harder to detect as attackers use more proxy servers and bots on legitimate IP addresses.
- **The X-Forwarded-For (XFF) HTTP header** identifies the source IP address of a client connecting to a web server through an HTTP proxy server, however, this header can be easily faked.
- **A browser's user agent** (a string in the HTTP header that identifies the browser and operating system to the web server the client is trying to connect to) also can easily be faked by bots.

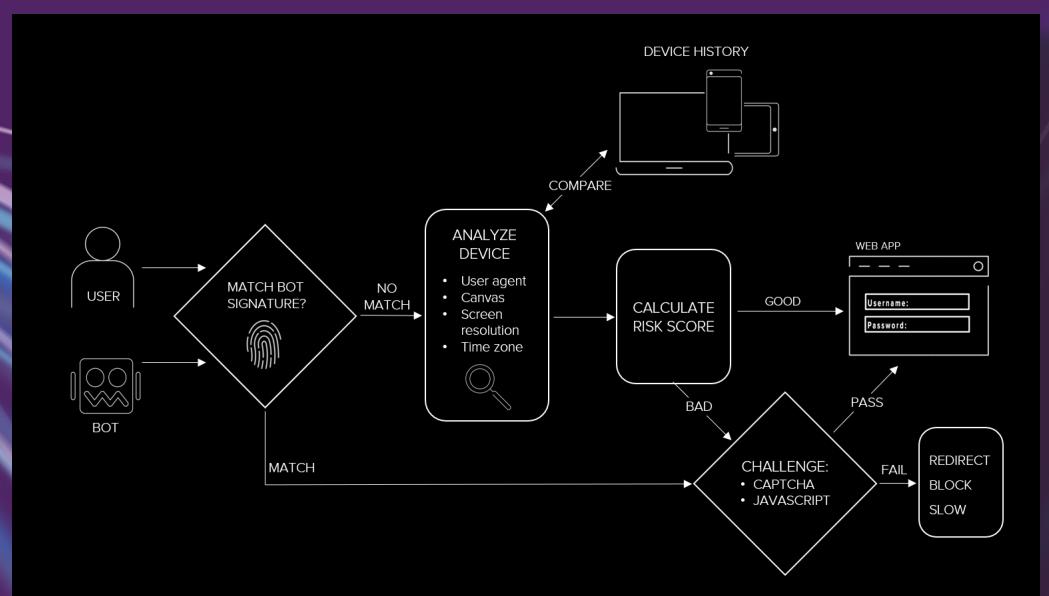
What's Good at Detecting Bots

The following methods are very good at detecting bots:

- **Bot signatures** identify web robots by looking for specific patterns in the headers of incoming HTTP requests. They can help you identify bots by type so you can decide what action to take (report, block, redirect, rate-limit, do nothing, etc.), and they have a low rate of producing false positives. Signatures for known malicious bots (e.g., DDoS attacks, scanners) must be updated regularly, and you can write your own bot signatures, as well.
- **Device fingerprinting**, a process used to identify a device (browser, laptop, tablet, smartphone, etc.) based on its specific and unique configuration, can be used to single out atypical behavior.
- **Browser attributes and behaviors.** Examining a browser's user agent declaration isn't sufficient, so it's more helpful to look at the difficult-to-spoof aspects of a browser such as:
 - > Browser plugins that are loaded and active. (Are any of them known hacking tools?)
 - > Screen resolution. (Is it reasonable, given a typical customer and client computing type?)
 - > Canvas. (Does it reasonably match the resolution?)
 - > Use contextual information to Identify repeating customers by learning their traffic patterns based on browsers they've used in the past and their typical times and locations of usages.

All of this data can feed a risk model that provides a score based on how much you know and trust that a connection is coming from a customer or a bot.

FIGURE 27: Methods for distinguishing bots from humans



68%

OF MALWARE USES
ENCRYPTION TO HIDE

Bot Detection Responses

When the risk scoring model reaches a threshold at which a bot is suspected, you have several options.

- **Issue a CAPTCHA challenge.** Note that some websites do this for all users, which can be off-putting to legitimate customers. In this case, you are issuing the challenge in response to analysis and once done, the user's profile can be added to the model so the connection need not be challenged again.
- **Issue a JavaScript challenge,** which doesn't bother the user because it runs silently in the browser. This JavaScript helps verify that a normal browser is being used. [Most bots cannot respond to a JavaScript challenge](#), so if the browser sends back a response, the traffic is legitimate.
- **Slow things down.** If a particular client appears bot-like but you'd prefer not to drop the traffic, you can use rate limiting to set a predetermined threshold for requests. This works well for dealing with the push/pull of a lot of requests coming from an apparent single origin. For example, are these hundreds of client connections coming at once because all the customers are at the same large organization (same originating IP and browser characteristics), or is it a credential stuffing attack? Until you figure it out, slow it down to contain the potential damage without driving away customers.
- **Redirect the traffic.** Another strategy for gray-area scores is to move the traffic away from the main site to either a maintenance page or to a limited functionality site. Legitimate customers will be inconvenienced but hopefully still come back later. Bots will likely give up and move on to a new victim.
- **Drop or block traffic** if you're pretty sure this is a bot based on the pattern. In fact, don't just block it here and now. Drop and block it forever, wherever you see it. You've now identified a new malicious pattern, so add it to your signature list.

Inspect Encrypted Traffic for Malware

Malware authors realized many years ago that traditional traffic inspection devices didn't decrypt traffic. This gave malware an invisibility cloak against scanning, simply by using SSL/TLS on the sites the malware was phoning home to. Of the malware domains Webroot identified to be active in September and October of 2018, 68% of them were taking traffic on port 443 (https). Traffic from malware sites communicating with command and control (C&C) servers over encrypted tunnels is completely undetectable in transit without some kind of decryption gateway. This is significant to enterprise environments that rely on malware infection notifications from intrusion detection devices, which cannot analyze encrypted traffic. Malware simply carries on collecting data and spreading undetected.

Phishing Incident Response

Security teams will have different incident response procedures depending on who's been impacted by a breach.

When customers' credentials are stolen, do the following:

- Send out notifications to customers warning them to beware of phishing attempts and include sample screen shots of the actual email. Advise employees who might have clicked on the email to call the help desk immediately.
- Immediately reset the passwords of impacted users.
- Advise customers to verify their transactions.

When a company's own users report a phish or have been phished, do the following:

- Don't blame the user; they were tricked by a professional. Instead, thank them for reporting it.
- Assume that other users got the same phishing email and opened it, clicked on a link, or opened an attachment.
- Scan your email system for the phishing email and remove it from all mailboxes. There is a decent chance it's still in the mailboxes of employees who haven't seen it yet, and you don't want to run the risk of someone else opening it once you know it exists.
- Reset the passwords of all impacted users.
- Send out warning to all employees with details on the specific lure.

FIGURE 28: An example of a security alert sent to F5 employees from the Security Awareness team

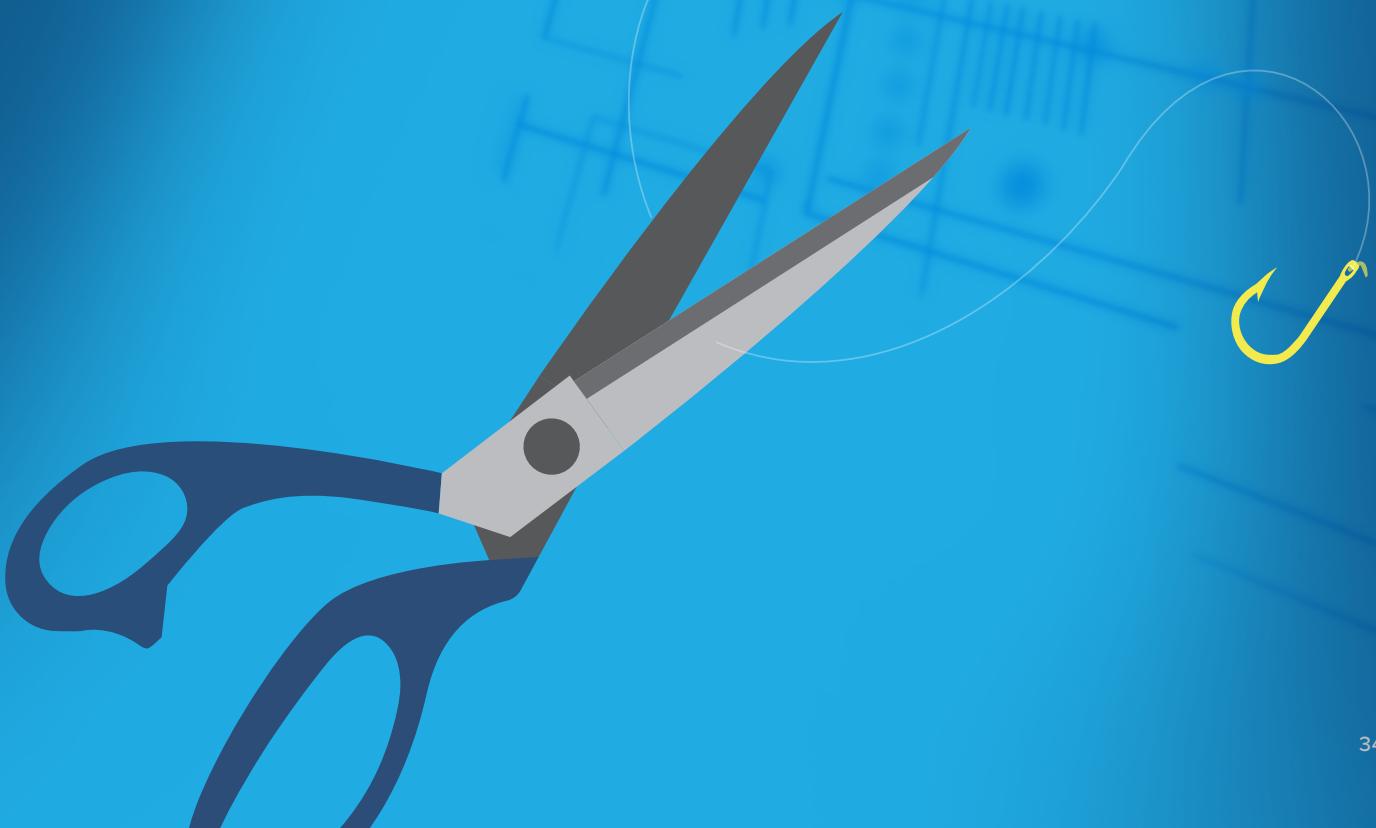


Information Security Alert

06/06/2014

<p>Security Awareness</p> <p>In This Issue</p> <ul style="list-style-type: none"> • Alerts! • What to do <p>More Information on Phishing</p> <p>Learn More About Phishing</p> <p>How to Avoid Scams</p> <p>Contact Us F5 Information Security</p>	<p>IT Security has recently received reports of fraudulent e-mails that have the appearance of being sent from a person you know (you will be in their email contact list). The e-mail exhibits various subject lines but contains a picture that you are enticed to open. The intent of the email is to collect personal or confidential information and to load malicious software onto end users' computers. If you open the picture or attachment, malicious software is installed on your computer.</p> <p>If the attack succeeds, the next time you visit a financial institution such as a bank or credit union you will see a pop up window asking you to fill out personal information such as Mother's maiden name, Social Security Number, driver's license and state of issue, and other sensitive information. Most financial organizations will not ask for this type of information on a web form, and you should not fill out such forms.</p> <p>Some warning signs most common to fraudulent malicious emails:</p> <ul style="list-style-type: none"> • Multiple recipients in the "To:" field. • Lack of personalized information. No partial account numbers, names, etc. • Mismatch of hyperlinks with destination. Example: the underlined text says "mybank.com" but the link destination takes you to "mybank.org" <p>If you see such an email to your f5.com account or a pop up screen from your F5 corporate machine when visiting your bank or financial institution, close it and report the issue to F5 IT Security and/or IT HelpDesk team immediately</p>
--	---

- Review access logs to see who might have already clicked on the phish and what damage has resulted from it.
- Keep the statistics on the event for executive reporting. Never let a crisis go to waste. The measured cost and potential damage of a phishing attack is an immensely useful statistic to track when justifying risk expenditures in the future. Even if a successful blunting of an attack can demonstrate the value of your existing solution and process. But you need to track that information so you can report on it later.
- Capture images of the phish for security awareness training later. Nothing brings training home for users like when you show them real attacks against real folks in their organization. It's hard to say "it can't happen here" when you can show them that it already has and they need to be ready for more.



Conclusion

Phishing attack? Absolutely.

Success? Likely.

Risk of incident? High.

Breach costs? About \$6.5 million.

No matter how you slice it, preventing a breach through security controls referenced in this report—including the hours it takes to train employees—is always cheaper than the cost of dealing with a breach.

But, be aware that multiple phishing breaches can occur in one year, and phishing attacks often compound on each other: a mailbox gets phished and then the attacker uses that compromised mailbox to phish more people, impersonating the first victim. It gets real messy, real fast. And dealing with phishing breaches is much different from dealing with breaches that happen through an application vulnerability, which are likely fixed during the normal incident response process. Phishing is a social engineering attack. You can't apply a patch to someone's brain (at least, not yet) or firewall off their ability to click on links or attachments in email, otherwise email would cease to exist as designed.

We expect phishing attacks to continue because they are so effective, both from the standpoint of their probability of success and the massive amounts of data they collect. As organizations continue to get better at web application security, it will be easier for fraudsters to phish people than to find web exploits. Therefore, it is critical to cover phishing attacks from both an administrative and a technical perspective as we laid out in the Defending Against Phishing and Fraud section of this report.

The recommended security controls list might seem extensive, but it's important to keep in mind that phishing attacks are designed to either trick users to give up their credentials or to install malware. Once inside the network, malware is designed to trick administrators. So, yes, the security controls are extensive. There is no one-stop-shop security control for phishing and fraud. A comprehensive control framework that includes people, process, and technology is a requirement to reduce the risk of a phishing attack becoming a major incident to your business.

ENDNOTES

¹ <https://r-cisc.org/blog/2018/09/>

² <https://retailleader.com/c-suite-role-every-retailer-needs>

³ <https://www.justice.gov/opa/press-release/file/1092091/download>



APPLICATION THREAT INTELLIGENCE



US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

©2018 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of the respective owners with no endorsement or affiliation, expressed or implied, claimed by F5. RPRT-SEC-283454530 | 0118