appgate

WHITEPAPER

HOW FRAUDSTERS EXPLOIT HUMAN BEHAVIOR TO CREATE INCREASINGLY SOPHISTICATED ATTACKS

Cybercriminal attacks are more complex than ever, and why only a multi-layered security strategy can stop them

For about as long as there has been the Internet, there has been the threat of attacks that exploit human behavior, such as phishing. The ease with which phishing attacks are developed and executed makes them a low cost, lucrative option for cybercriminals. Whether it's through business email compromise, social media impersonation, or any other type of phishing attack, organizations and their brands are constantly at risk. The monetary and long-term reputational damage of a major attack can greatly weaken any institution. This whitepaper will examine various examples of successful phishing attacks against large companies and explain how strong, multi-layered security strategies can protect organizations from crippling financial and reputational losses.

THE CURRENT STATE OF PHISHING

Phishing has been around for decades and shows no signs of disappearing any time soon. Most attacks and data breaches start with some type of phishing attack, and there was a 250% increase in phishing websites in 2016. The total number of phishing attack types recorded by the APWG in 2016 was 1,220,523, an all-time high and a 65% increase from 2015.[1]

Why is phishing at an all-time high? With low operational costs, minimal technical knowledge required, and a high return on investment, criminals continuously turn to phishing to make profits. The attack itself normally stems from social engineering. It uses not just technology but also human weakness; though technology can evolve, the human factor of an attack always remains the same. Further, enterprises, especially banks, have learned to create lines of defense from within the perimeter. Phishing, on the other hand, exploits the link outside of the perimeter: the user. Organizations often don't protect end users or their devices, and vectors such as email and social media remain completely unprotected.

Most attacks and data breaches start with some type of phishing attack.

a
FORTUNE
Yahoo CEO Marissa Mayer Just Lost Her Bonus
b
Forbes
Target's CEO Steps Down Following The Massive Data Breach
c
SECURITY WEEK
Austrian Firm Fires CEO After $56-million Cyber Scam
d
CSO
The reputational damage of data breaches: don't hope for customer apathy

Figure 1: Phishing Attack Headlines

- http://fortune.com/2017/03/02/marissa-mayer-yahoo-bonus/
b- https://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-and-canadian-debacle/#7322075e2ba6
c- http://www.securityweek.com/austrian-firm-fires-ceo-after-56-million-cyber-scam
d- https://www.cso.com.au/blog/cso-bloggers/2015/10/29/the-reputational-damage-of-data-breaches-dont-hope-for-customer-apathy/

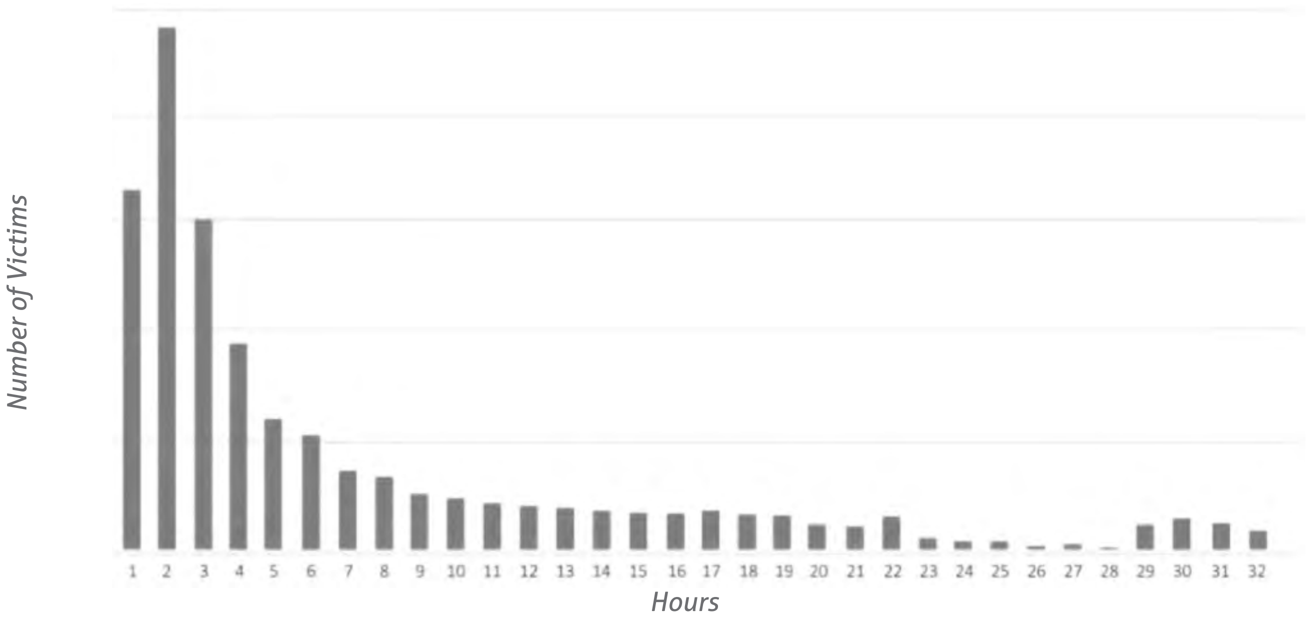
[1] http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

ATTACKERS EXPLOIT HUMANS, NOT CODE, TO STEAL FUNDS

It is becoming increasingly difficult for end users to determine if news, social media pages, emails, and other content are from legitimate companies or cybercriminals. As digital attacks become more sophisticated and targeted, organizations face increasing pressure to protect their brands and their customers.

Ninety-seven percent of people don't know how to accurately recognize a phishing email, and 30% of phishing emails are opened. Even scarier, there were 13,000 new phishing sites created daily in 2016, and over 400,000 fraudulent sites were visited every month. When these attacks are successful, the most damage occurs right after the site's launch - the vast majority of attack victims visit a phishing site within the first few hours, and researchers have determined that 70% of credentials are collected within the first few hours of a phishing attack.[2]

70% of credentials are collected within the first few hours of a phishing attack.

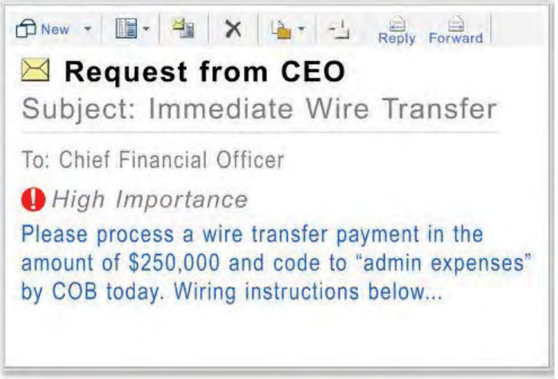


Internal data compiled by Easy Solutions

Figure 2: Number of Victims Per Hour

from January 2015 to December 2016. BEC is a form of spearphishing in which attackers pretend to be an executive or financial officer at a company in order to convince employees to transfer large sums o money to the hacker's account. The FBI Internet Crime Complaint Center reported that between October 2013 and June 2016, BEC cost companies over $5.3 billion USD.[3]

In August 2016, an employee in the finance department of the European manufacturing company Leoni AG received an email that appeared to be from one of the company's executives. This email requested a transfer of funds out of the company's bank account; the attackers were able to make the email so convincingly real that the employee completed the transaction. This simple attack resulted in a €40 million Euro loss for the company. Adding insult to injury, the company's stock lost 7% of its value as customers began to lose trust in the brand.



Request from CEO

Subject: Immediate Wire Transfer

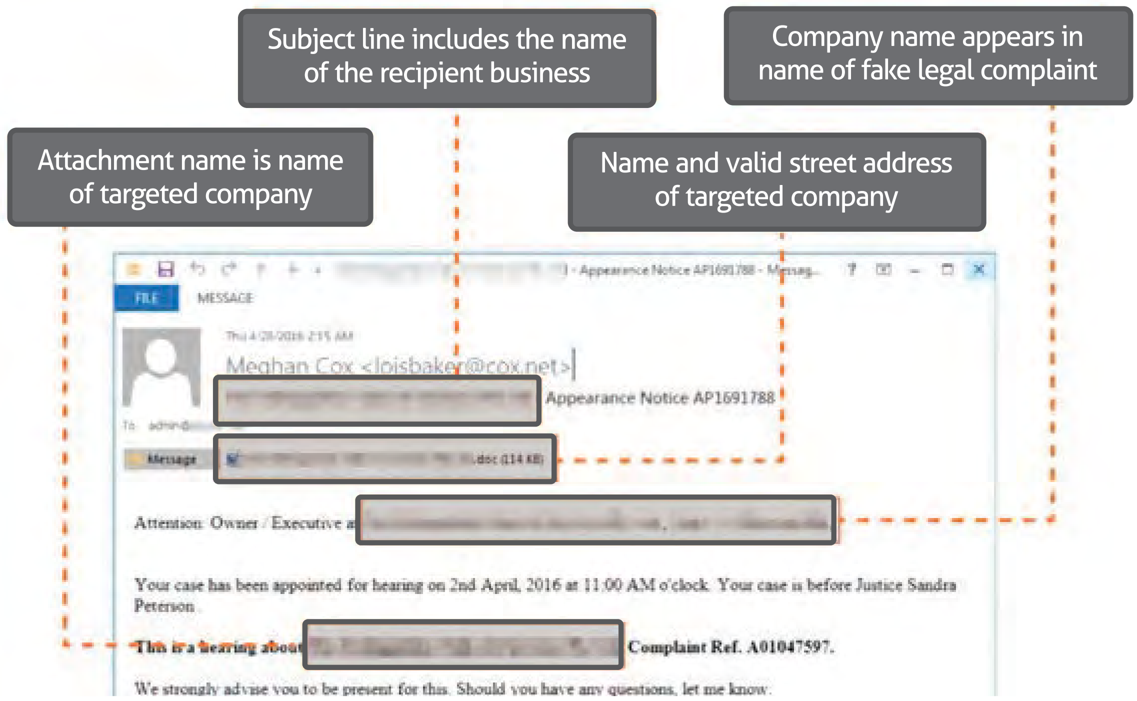
To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

[2] https://securityintelligence.com/phishing-attacks-collect-70-percent-of-credentials-within-the-first-hour/

[3] https://www.ic3.gov/media/2017/170504.aspx



Subject line includes the name of the recipient business

Company name appears in name of fake legal complaint

Attachment name is name of targeted company

Name and valid street address of targeted company

Thu 4/28/2016 2:15 AM

Meghan Cox <loisbaker@cox.net>

[redacted] Appearance Notice AP1691788

To admin@[redacted]

[redacted].doc (114 KB)

Attention: Owner / Executive a[redacted]

Your case has been appointed for hearing on 2nd April, 2016 at 11:00 AM o'clock. Your case is before Justice Sandra Peterson.

This is a hearing about [redacted] Complaint Ref. A01047597.

We strongly advise you to be present for this. Should you have any questions, let me know.

NOT JUST YOUR DATE IS AT RISK

IIn May 2017, a sophisticated phishing attack hit Google: Gmail users were sent emails that appeared to be from legitimate contacts, prompting them to open a Google Doc that had been shared with them. When they went to open the doc, they were prompted to give the "Google Doc" application permissions. However, this app was actually a fake, and was used to access users' contacts and send messages to further perpetuate the scam.

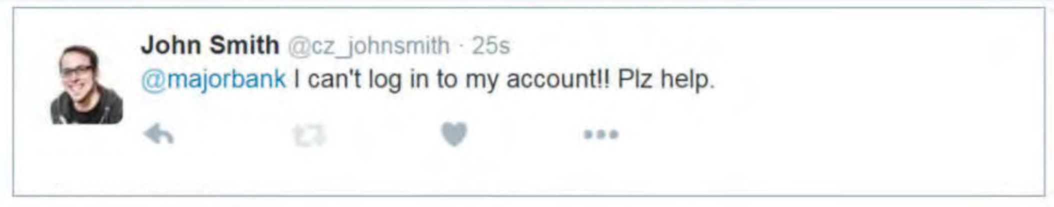
While this attack was not used to steal money or other information, it did cause security issues for Google, resulting in extra costs for the company. Fixing the problem and creating security updates required financial resources and used up valuable employee time.

Another major attack took place against Sony Pictures in 2014. Hackers stole large amounts of data including unreleased movies, emails, and scripts for future productions in a hack that could have been prevented, or at least the effects reduced, if the company had had stronger security mechanisms in place. The financial and reputational impact of the attack was immense. The company lost revenue from ticket sales for movies that were released online before they hit theaters, and the premiere of one movie was even canceled. Customers lost faith in the integrity of the company, and, as a result, became less loyal to Sony as a brand.[4]

SOCIAL MEDIA IMPOERSONATION IS ON THE RISE

Our final fraud vector is social media impersonation - when fraudsters pretend to be representatives of a brand on social media in order to lure users into giving them sensitive information.

PayPal fell victim to this in on Twitter in 2016. Customers often turn to social media, especially Twitter, to resolve service questions, and this happens often with PayPal. In this attack, the fraudsters answered clients' questions from fake accounts and, in doing so, redirected these customers to non-legitimate websites. Those websites claimed to be the official PayPal website in an attempt to convince users to input their account information to then steal their log-in credentials.

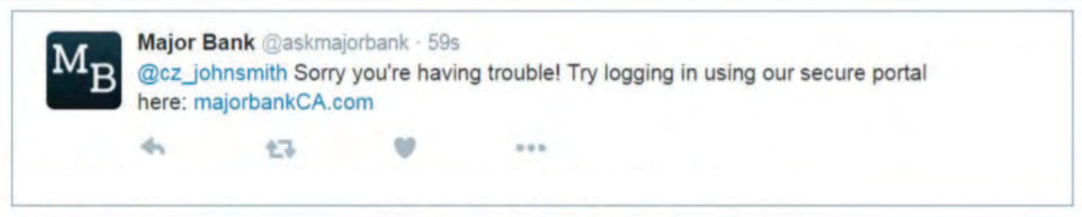


John Smith @cz_johnsmith · 25s

@majorbank I can't log in to my account!! Plz help.

Figure 5: Social Media Impersonation

Since many companies have various Twitter accounts to respond to inquiries from different regions or customer sub-sets, users are unlikely to become alarmed when they receive a response from an account that is different from the account they originally wrote to. As PayPal had no security measures in place to take down accounts perpetuating this type of fraud, it left its customers at high risk of falling victim to this scheme. As with all financial institutions that conduct transactions online, trust is incredibly important to the PayPal brand. When customers are at risk of losing money to these scams, they turn to other, more secure, methods of making online payments.



Major Bank @askmajorbank · 59s

@cz_johnsmith Sorry you're having trouble! Try logging in using our secure portal here: majorbankCA.com

Figure 6: Social Media Impersonation

MORE THAN JUST MONETARY LOSSES

As with Google, Sony, and PayPal, your brand is at risk if you are unprotected. Not only will your customers lose trust in your brand, it may be you who personally pays the price of the consequences of an attack. Your job may be at risk, as well as the well-being of your organization.

The losses to fraud are by no means definite; financial losses are clear, and the amount of money lost to the fraudsters is set. However, damage to the brand is more difficult to quantify and even more difficult to recover from. Not only must you recover from the monetary losses, but you also have to deal with consumers choosing to go elsewhere to do their business where they feel more secure. The damage caused by a fraud attack isn't just measured in the monetary losses to the scam - 83% of organizations that suffer fraud incidents experience loss of clients, reputation, and/or productivity.[5]

The damage caused by a fraud attack isn't just measured in the monetary losses to the scam 83% of organizations that suffer fraud incidents experience loss of clients, reputation, and/or productivity.

[5] Faces of Fraud: The 2016 Agenda-http://f6ce1404647f05e937f4-4d6abce 208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/faces-fraud-2016-agenda-pdf-6-w-2217.pdf

WHAT DO EXPERTS SAY?

Having a strong security plan in place can help you rest assured that your company is not at risk of suffering from a phishing attack that results in severe damage to your brand.

Experts recommend that companies go above and beyond just focusing on behavioral management of employees, or simply teaching them how to detect spoofed emails, when fighting phishing. Phishing relies on social engineering tactics to trick victims into believing that they are accessing legitimate emails, websites, or other content. As cybercriminals advance in their phishing techniques, employees and customers cannot be relied on as a strong defensive strategy against phishing, and technology must adapt to increasingly sophisticated attack strategies. Leading experts and fraud security industry analysts agree that the following recommendations can help companies avoid falling victim to phishing and other kinds of cyberattacks:

- Implement an anti-fraud solution that monitors online brand mentions and activity to prevent your organization's name from being used in a harmful or malicious manner.
- Strengthen detection capabilities, such as employing machine learning technology, to ensure that attacks do not go unseen.
- Utilize multi-factor end-user authentication to minimize the damage of successful account breaches. - Deploy an email authentication protocol, such as DMARC, to prevent spoofed messages from reaching employee or customer inboxes.
- Set in motion a strategy to efficiently detect and remove phishing websites.

Traditional security strategies are no longer effective in the evolving threat landscape. In order for companies to stay completely protected, it is imperative to implement a multi-layered, intelligent fraud protection strategy that is constantly adapting to new and advanced threats.

CRIMINAL CONSTANTLY ADAPT TO NEW SECURITY MEASURES

As more anti-phishing security measures are put in place, we see an increase in highly sophisticated and targeted attacks. While the overall volume of these attacks is relatively low, their targeted nature makes them much more dangerous and effective. An example of this is the homograph attack which exploits Unicode, an encoding standard that allows for the use of different languages and scripts in the creation of domain names and turns them into unique combinations of letters and numbers.

For many years, cybercriminals have created fake domain names that are very similar to legitimate names in order to trick users into thinking that they are using a legitimate website. Normally, this change involves just one character or word, but can be detected by a trained eye. However, there are always workarounds that allow attackers to be even more creative when creating fake URLs. It was recently exposed that criminals can, and have, leveraged vulnerabilities in some browsers when registering domains with non-Latin characters using Unicode. Attackers can use characters from other alphabets to make it appear as if a domain name is legitimate: though the URL looks as if it is spelling out a word in Roman characters, it is, in fact, a completely different word.

For example, the domain below appears to link to the website for Apple. However, upon further examining the URL, it becomes clear that the URL actually uses Cyrillic characters that look almost identical to Latin characters.

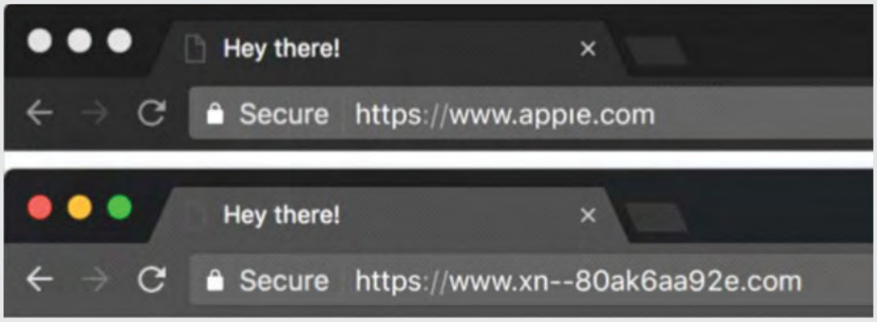


Figure 7: Example of a Homograph Attack

DIGITAL THREAT PROTECTION

Digital Threat Protection continuously analyzes and monitors a wide range of sources across the web, including social media, email, news, forums blogs, and more in search of phishing and other online attacks. This extensive coverage results in unmatched visibility. Through its unique detection intelligence capabilities, evidence of phishing and other attacks are found and confirmed by using different proprietary machine learning classification algorithms. Identified threats are rapidly removed before customers and employees are aware of any disruption. Digital Threat Protection is a proven solution that has monitored over 30 billion connections, analyzed more than 50 million suspicious emails, and discovered more than 385,000 phishing attacks and rogue apps per year. Appgate has an average mitigation time of 10 minutes and 70% of the time, an attack is detected before customers are or their employees are aware of it. By taking a proactive approach to fighting fraud, attacks can be combatted before they are even executed, decreasing attack volume and allowing financial institutions to focus on the future, not the fear of fraud.

Digital Threat Protection from Appgate combines the DMARC (Domain-based Message Authentication, Reporting, and Conformance) standard with DMS (Detect Monitoring Service) to provide comprehensive protection for your company.

DMARC, which is built upon the SPF and DKIM protocols, allows companies to monitor who is sending spoofed emails, who is receiving those emails, and which servers are responsible for sending them out with a DMARC policy in place, emails that do not come from a company's server never even reach inboxes, vastly reducing phishing messages.

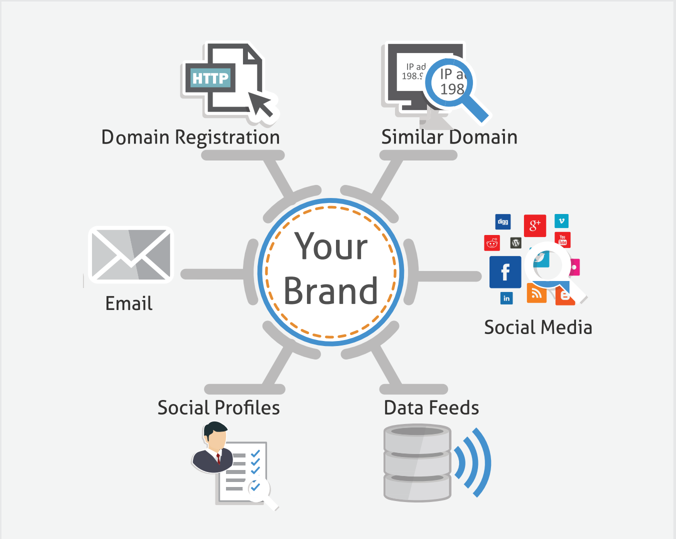


Figure 8: Aspects of Your Brand

DMS is a 24/7/365 service that provides early phishing detection across the web, social media, and email sources. It analyzes social media networks to find and report fake social profiles or other domains impersonating legitimate companies. It then takes down threats before your customers or employees even become aware of their existence. New phishing campaigns are launched daily and through various mediums, so it is important to have a proactive anti-phishing strategy in place. As attacks are most effective within the first few hours of their launch, anti-phishing strategies must be able to quickly and efficiently detect and completely remove threats.

WHAT DIGITAL THREAT PROTECTION CAN DO FOR YOUR ORGANIZATION

The Digital Threat Protection suite offers a variety of benefits to businesses, including:

UNMATCHED VISIBILITY

Continuous analysis and monitoring of a wide range of sources across emails, web, and social media channels with custom dataset integration like DMARC reports, abuse box, and referrer weblogs.

UNIQUE DETECTION AND INTELLIGENCE

Quickly finds and confirms evidence of phishing and other attacks at scale by using different proprietary machine learning classification algorithms.

EXPEDITED ATTACK TAKEDOWN

Rapidly removes identified threats before customers or employees become aware of a threat's presence.

CONVENIENT ADOPTION

An outsourced service means simple setup, no integration required, and minimal resource investment.

REDUCE EMAIL FRAUD

Block business email compromise and email spoofing of your domains before they affect your employees and customers.

COMPREHENSIVE REPORTING

Cloud portal allows users a real-time view of all of the aspects of your digital threat protection strategy. The online dashboard illustrates threat data and allows users to receive alerts and request takedowns.

appgate