THE COST OF CYBERCRIME TO BUSINESSES OVER THE NEXT FIVE YEARS IS EXPECTED TO BE US $8 TRILLION.¹

**ROOT CAUSE**

Phishing is the root cause in over 95 percent of breaches. Sophisticated phishing campaigns assault businesses across all vectors: email, web, and network, resulting in theft of intellectual property, data loss, financial damage, brand erosion, and ongoing harm to the brand. Existing defenses have failed to eliminate phishing because they are:

- Focused on general email spam or web compliance
- Reactive and unable to identify small but key patterns
- Siloed on individual delivery methods and not comprehensive
- Focused on awareness rather than decisive deterrent action

The lexicon describing cybersecurity threats has exploded, creating confusion as well as hampering action towards achieving measurable results. Attacks such as BEC, whaling, ransomware, and watering hole are all caused by phishing. These attempts to lure users into opening emails, clicking on links, downloading files, transferring money or data, and entering information such as passwords into websites should be identified and defined by their intent, and not technical method or the effect they cause. **All are forms of phishing.**

---

Over 200 virus varieties cause the common cold. The rhinoviruses, with 99 recognized types, are the most common. Other viruses include coronavirus, parainfluenza, adenovirus, enterovirus, and respiratory syncytial virus. Vaccinations for viruses focus on commonalities among them, and not on distinctions that differentiate them. **The same rationale applies to cybersecurity.**

---

1 https://www.cdc.gov/getsmart/community/for-patients/common-illnesses/colds.html
Overall, Verizon’s findings show that 90% of data breaches have a phishing component.\(^2\)

**THE NUMBERS**

We see many statistics that rank phishing in the 90th percentile as the cause of data breaches. Regardless of the true percentage point, phishing is clearly the most effective method of hacking, with the most severe consequences.

Even the most credible statistics may employ different terms to describe what is essentially the same thing. This can distract customers from attacking the root cause of their problem and instead focus their attention—and their dollars—on solving symptoms.

However, careful data analysis shows that the aggregate meaning of the statistics is clear and consistent, namely: phishing is the #1 attack vector in cybersecurity and is overwhelmingly responsible as the root cause of breaches. The largest firms conducting incident response to the most damaging attacks worldwide report that 97 percent of their investigations identify phishing as the initial attack mode (the remaining 3 percent have an unidentified root cause). The Verizon Data Breach Investigations Report (DBIR) provides granular statistics, such as:

- 66% of malware is installed via malicious email attachments
- 81% of hacking-related breaches leverage either stolen and/or poor, weak passwords
- 43% are social attacks
- 21% of breaches are related to espionage

A phishing attack is a phishing attack, so we treat it as such. We combine all these subcategories and look at phishing campaigns as a whole. This is where businesses should focus and apply their resources.
The industry's top anti-spam companies claim, via their invoices, that they catch 99 percent of unwanted traffic directed to their clients' inboxes. While that missing one percent may seem minimal, it actually represents 100 percent of the damage experienced by companies who neglect that seemingly insignificant percentage point.

Widespread media frenzy over these two ransomware attacks distracts people from the larger and far more important issue: phishing itself. WannaCry and Petya actually stole very little money or data—compared to targeted phishing attacks, in which a single click can cost an organization many times the damage of WannaCry and Petya combined.

---

2 Verizon 2017 Data Breach Investigations Report
TOP CYBER ACTORS USING PHISHING

CASE STUDIES OF PHISHING ATTACKS
NSA’s TAO Chief Speaks on Disrupting Nation State Hackers at Enigma Conference 2016

“Contrary to popular opinion,” says Rob Joyce, Chief, Tailored Access Operations, National Security Agency, “the NSA and other APT attackers don’t rely on zero-day... hackers are more likely to use phishing attacks... it is necessary to implement security controls that do not rely on users to do the right thing.”

TOP 7 CYBER ACTORS USING PHISHING

01 NETWORK HACK PROGRAM HACKER GROUP AKA NCPH GROUP

PROMINENT CAMPAIGNS
Earned a reputation among cyberattackers by hacking 40% of Chinese hacker association websites.

ASSOCIATED DAMAGE
Responsible for zero-day hacker "proof-of-concept" codes used in attacks over 90 days during summer 2006.
TURLA  AKA  SNAKE

PROMINENT CAMPAIGNS
US Central Command in 2008, RUAG (Swiss military contractor).

ASSOCIATED DAMAGE
Extracted data from government or government-sponsored organizations.

CARBANAK  AKA  FIN7

PROMINENT CAMPAIGNS
Stole $1B from independent banks across Russia and other countries.

ASSOCIATED DAMAGE
Stole between $500M-$1B from banks and 1,000+ private entities.
POTASSIUM / RED APOLLO AKA APT10

PROMINENT CAMPAIGNS
One of the largest sustained global cyber espionage campaigns against firms in the UK, Japan, France, and the US.

ASSOCIATED DAMAGE
Exfiltrated high volume of data from multiple victims. Used compromised networks to stealthily move this data around the world.

GUARDIANS OF PEACE

PROMINENT CAMPAIGNS
Responsible for the Sony data breach. Used spear-phishing to access internal servers by targeting employees asked to verify their personal Apple IDs.

ASSOCIATED DAMAGE
Several internal data centers wiped clean: led to cancellation of movie release, stolen contracts, salary lists, film budgets, entire films, and Social Security numbers. Leaked emails criticizing Angelina Jolie and then-President Obama.
BUHTRAP

PROMINENT CAMPAIGNS
Attack on Bangladesh’s central bank controlling access to the SWIFT messaging system.

ASSOCIATED DAMAGE
Yielded more than $81M — one of the biggest digital heists on record. Hit ATMs in Taiwan and Thailand. Russian banks lost over $28M in wire-fraud cases.

$81M

SOFACTY AKA APT28

PROMINENT CAMPAIGNS
Masqueraded as NATO representative; sent phishing emails to European diplomatic organizations, including Romania’s Foreign Ministry of Hacking.

ASSOCIATED DAMAGE
Likely led to information exfiltration from multiple senior party members.
MOST DAMAGING DATA BREACHES OF THE PAST

FIVE YEARS

Target

DECEMBER 2013

The retail giant initially announced that hackers had gained access by phishing through a third-party HVAC vendor to its point-of-sale (POS) payment card readers, and had collected about 40 million credit and debit card numbers. These included full names, addresses, email addresses, and telephone numbers. The final estimate is that the breach affected as many as 110 million customers.3

JP Morgan Chase

JULY 2014

Seventy-six million households and 7 million small businesses were the victims of a phishing attack on the massive bank during the summer of 2014 that compromised the data of more than half of all US households. Stolen data included contact information—names, addresses, phone numbers, email addresses—as well as internal information about users.4

Sony

NOVEMBER 2014

A massive phishing attack targeted employees who were asked to verify their Apple IDs. This caused several internal data centers to be wiped clean and led to the cancellation of the release of the movie, The Interview, a comedy about a fictional assassination attempt on the North Korean leader. Contracts, salary lists, film budgets, entire films, and Social Security numbers were stolen. The heist included leaked emails that criticized Angelina Jolie and made disparaging remarks about then President Obama.5

Premera Blue Cross

MARCH 2015

Health insurer based in Washington said that up to 11 million customers could have been affected by a wave of phishing emails. The breach exposed members’ names, dates of birth, Social Security numbers, mailing and email addresses, phone numbers, and bank account information. Attacks may be linked to a state-sponsored attack originating in China.6

OPM Data Breach

Phishing emails were sent to US government employees in order to gain access to the Office of Personnel Management. An estimated four million government employees had all of their information, even Social Security numbers, exposed to hackers. Experts have warned that the danger is even more widespread, since those employees with a security clearance had to apply with a 100+ page form that called for highly detailed contact information on people the applicants knew who could vouch for them. This included former schoolmates, teachers, landlords, employers and colleagues, family members, and friends.7

2016 Presidential Election

Hillary Clinton’s campaign manager, John Podesta, received a phishing email masked as an alert from Google that another user had tried to access his account. It contained a link to a page where Podesta can change his password. He shared the email with a staffer from the campaign’s help desk. The staffer replied with a typo: instead of typing “This is an illegitimate email,” the staffer typed, “This is a legitimate email.” Podesta then followed the instructions and typed a new password, allowing hackers to access his emails. Many of his personal emails were leaked, causing widespread controversy.8

Citibank

Citibank phishing scam used advanced techniques to manipulate users into surrendering online banking access; it tricked users into surrendering their online banking username, password, and additional one-time pin (OTP) verification code. Like many phishing messages, the basic e-mail looked relatively authentic, with logos and images that were linked from the real Citibank site. The message asked readers to click on the button to check their accounts and report any suspicious or fraudulent account activity. If you clicked on the button, you were brought to an authentic-looking web page where you were asked to log on. If you did, they had you. While this site was only up for a day or so before being shut down, it may have netted victims because of the masked address. Over 200,000 credit cards were affected as a result of this attack.9

---

W-2 Tax Documents

Cybercriminals used various spoofing techniques to disguise an email, making it appear as if it came from an organization executive. The email was sent to an employee in the payroll or human resources departments, requesting a list of all employees and their W-2 forms. This phishing scam is sometimes referred to as business email compromise (BEC) or business email spoofing (BES). IRS Commissioner John Koskinen states, “This is one of the most dangerous email phishing scams we’ve seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone’s help to turn the tide against this scheme.”

Chipotle

On Feb. 22, a phishing email carrying an attachment titled “PaymentOverdue.eml” was sent to an email account associated with a Chipotle location in Tulsa, Oklahoma. The body of the phishing email described a nonexistent overdue payment and encouraged the victim to open a booby-trapped attachment. The email sender was listed as Michael Smith, an imaginary manager for a nonexistent company named Slazzer LLC. The malware-laden attachment in the email sent to the Tulsa-based Chipotle was a malicious Microsoft Office .RTF file with an embedded OLE object. As a result, many customer names and debit and credit card numbers were leaked to the hackers.

Facebook and Google

According to the Justice Department, a man forged email addresses, invoices, and corporate stamps in order to impersonate a large Asian-based manufacturer with whom the tech firms regularly did business. The point was to trick companies into paying for computer supplies. The scheme worked. Over a two-year span, the corporate imposter convinced accounting departments at the two tech companies to make transfers worth tens of millions of dollars. By the time the firms figured out what was going on, the man had coaxed out over $100 million in payments, which he promptly stashed in bank accounts across Eastern Europe.

OTHER NOTABLE PHISHING ATTACKS

Yahoo

The company released details in 2016 of a massive data breach that likely occurred in late 2014 as a result of phishing attacks directly before an acquisition deal was offered by Verizon. The announcement cost them a loss of $350 million from their initial valuation.

Locky Ransomware Campaign

In the wake of the OPM hacking, hacker groups have been playing off the fears of government workers by sending phishing emails that ask them to verify their personal information through malicious links. This information is then immediately stolen by the hackers.

Barclays BEC Attack

Barclays CEO Jes Staley received an email seeming to be from the bank’s chairman. In this case, a fake email was created by a hacker that fooled the CEO for a time. The hacker sent comical messages that ended in a poem that spelled out “whistleblower”. Although no serious damage was done, it is a great example of how easy it is to fall for an email sent from a seemingly trustworthy source.
**SUMMARY**

The large-scale attacks and disastrous outcomes in this paper underscore the fact that targeted phishing is the overwhelming cause of nearly all breaches. Phishing attacks cost companies an incalculable amount of money, prestige, goodwill, confidential data, and competitive advantage, as well as brand identity and integrity. The Verizon Data Breach Investigations report supports the overwhelming impact of phishing, which targets businesses consistently across email, web, and network traffic. Siloed approaches lead only to siloed and ineffective protection. Partial, reactive defenses such as employee education, perimeter protection, and spam filtering simply don’t work against today’s phishing threats.

In order to be effective, a solution must be comprehensive and able to stop attacks preemptively—while they are still under construction—rather than wait for them to arrive in users’ inboxes and deceive them into clicking on a malicious web link, divulging employee information, forwarding funds, or exposing intellectual property. When a single phish can inflict lasting damage on the entire company, as noted with the firms above; a comprehensive and preemptive defense model is not only critical to changing outcomes; it is the only approach that can work successfully.
ABOUT

The industry's most comprehensive anti-phishing solution, Area 1 Horizon™ stops phishing campaigns during the earliest stages of an attack cycle.

Backed by top tier investors, Area 1 Security is led by security and data analytics experts coming from NSA, USCYBERCOM, Cisco/IronPort and FireEye who realized a pressing need for a proactive solution to targeted phishing attacks. Area 1 Security works with some of the most sophisticated organizations in the world, including F500 banks, insurance companies, and health care providers, to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture, and change outcomes.

Learn more and get in touch with us for a free preview:
INFO@AREA1SECURITY.COM
arealsecurity.com

PHISHING /FIsh-ing/

n. Any attempt to unwittingly lure users to click links, download files, surrender data or expose financial assets.