PHISHING ACTIVITY TRENDS REPORT

2nd Quarter 2022

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2022

Published 20 September 2022

Phishing Report Scope

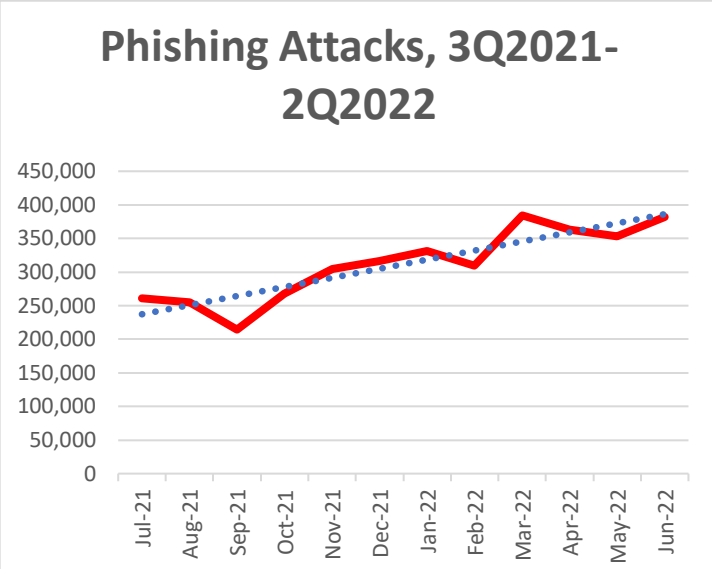
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG measures the evolution, proliferation, and propagation of identity theft methods by drawing from the research of our member companies and industry experts.

Phishing Defined

Phishing is a crime employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and email messages. These are designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to steal credentials directly, often using systems that intercept consumers' account usernames and passwords or misdirect consumers to counterfeit Web sites.

Table of Contents

Phishing Attacks Climb to New Record High in 2022



Phishing Activity Trends Summary

- In the second quarter of 2022, APWG observed 1,097,811 total phishing attacks, a new record and the worst quarter for phishing that APWG has ever observed. [pp. 3-4]
- The average amount requested in wire transfer BEC attacks in Q2 2022 was $109,467, up from $91,436 in Q1 2022. [pp. 8-9]
- The healthcare and transportation industries suffered an increase in ransomware attacks. [pp. 6-7]
- Threats on social media continued to rise, with a 47 percent increase from Q1 to Q2 2022. [pp. 11-12]
- There has been an increase in mobile phone based fraud, with smishing and vishing increasing in Q2 2022. [p. 5]

Statistical Highlights for the 1st Quarter 2022

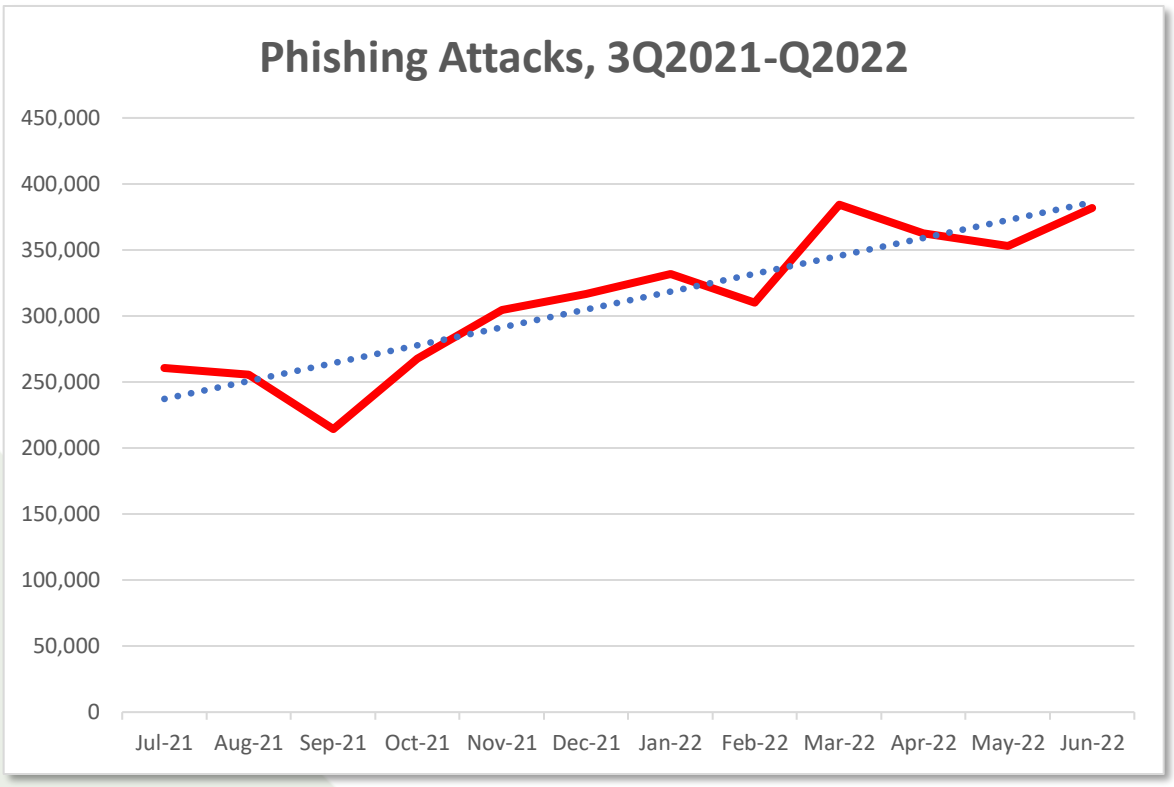
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. With this report, the APWG has refined the methodologies it uses to report phishing. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

The APWG tracks:

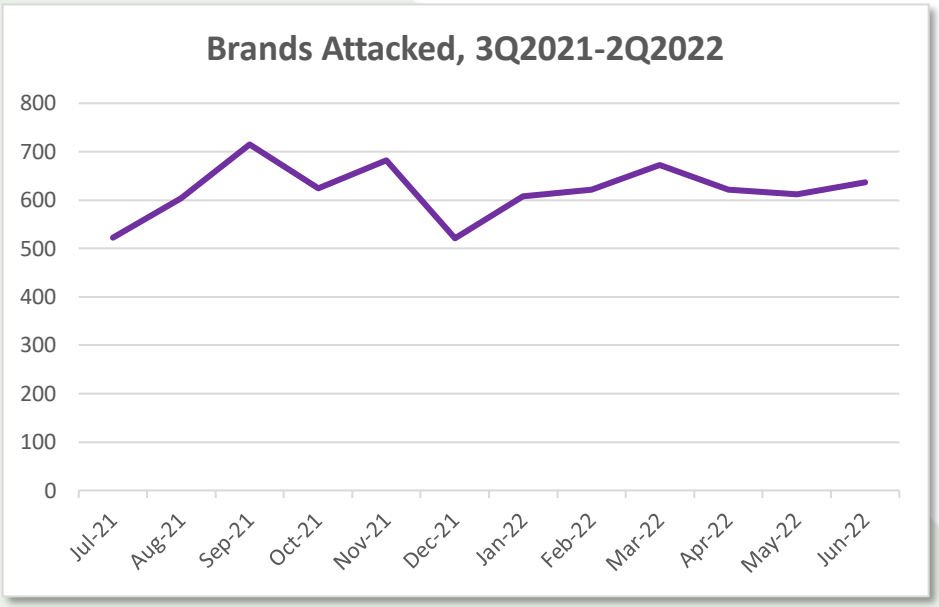
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same destination.) Thus APWG measures reported phishing sites, which is a more relevant metric than URLs. A synonym for sites is *attacks*.
- **Unique phishing e-mails subjects**. This counts email lures that have different email subject lines. Some phishing campaigns may use the same subject line but advertise different phishing sites. This metric is a general measure of the variety of phishing attacks, and can be a rough proxy for the amount of phishing taking place.
- The APWG also counts the **number of brands attacked** by examining the phishing reports submitted into the APWG eCrime Exchange, and normalizing the spellings of brand names.

	April	May	June
Number of unique phishing Web sites (attacks) detected	362,852	353,242	381,717
Unique phishing email subjects	21,540	20,339	23,550
Number of brands targeted by phishing campaigns	621	612	637

In the first quarter of 2022, APWG observed 1,025,968 total phishing attacks. **In the second quarter of 2022, APWG observed 1,097,811 total phishing attacks, a new record and the worst quarter for phishing that APWG has ever observed.** The number of phishing attacks reported to APWG has quadrupled since early 2020, when APWG was observing between 68,000 and 94,000 attacks per month.



The number of Unique Subjects grew as more submitted emails had differing subject lines. The number of brands attacked each month has remained below the high of 715 observed in September 2021:



Most-Targeted Industry Sectors – 2nd Quarter 2022

In Q2 2022, APWG founding member OpSec Security found that phishing attacks against the financial sector, which includes banks, remained the largest set of attacks, accounting for 27.6 percent of all phishing. Attacks against webmail and software-as-a-service (SAAS) providers remained prevalent as well, while attacks against retail/ecommerce sites fell from 14.6 to 5.6 percent. Phishing against social media companies rose, from 8.5 percent of all attacks in 4Q2021 to 15.5 percent in 2Q2022. Phishing against cryptocurrency targets — such as cryptocurrency exchanges and wallet providers — remained active, and were more prevalent than attacks against online games, government sites, and telecom services combined. Overall, OpSec detected a 43 percent increase in phishing compared to Q1 2022.

Matthew Harris, Senior Product Manager, Fraud at Opsec, noted: "Lastly, we're seeing a huge increase in mobile phone-based fraud, with smishing and vishing collectively seeing a nearly 70 percent increase in volume as compared to Q1 totals."

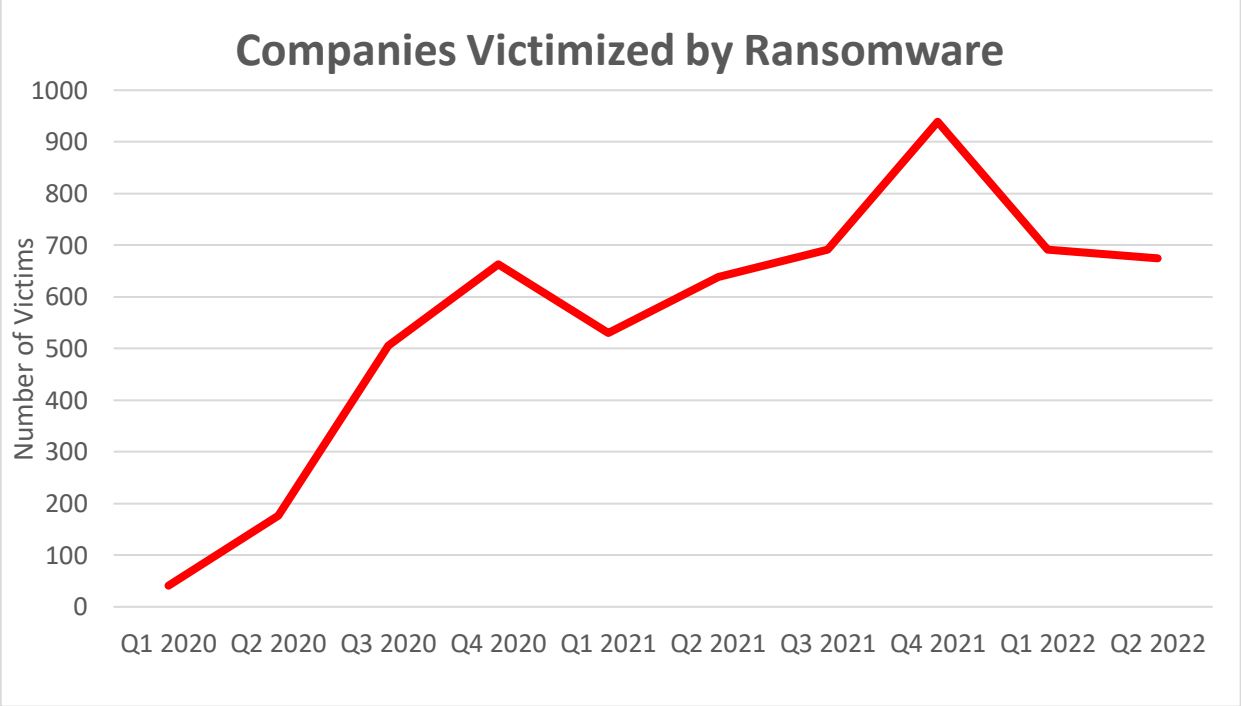
"We are still seeing fraud coming in via the typical OTT apps (WhatsApp, WeChat, Facebook Messenger, etc), but the SMS-based fraud is really the kicker here," Harris said.

OpSec Security offers world-class brand protection solutions.

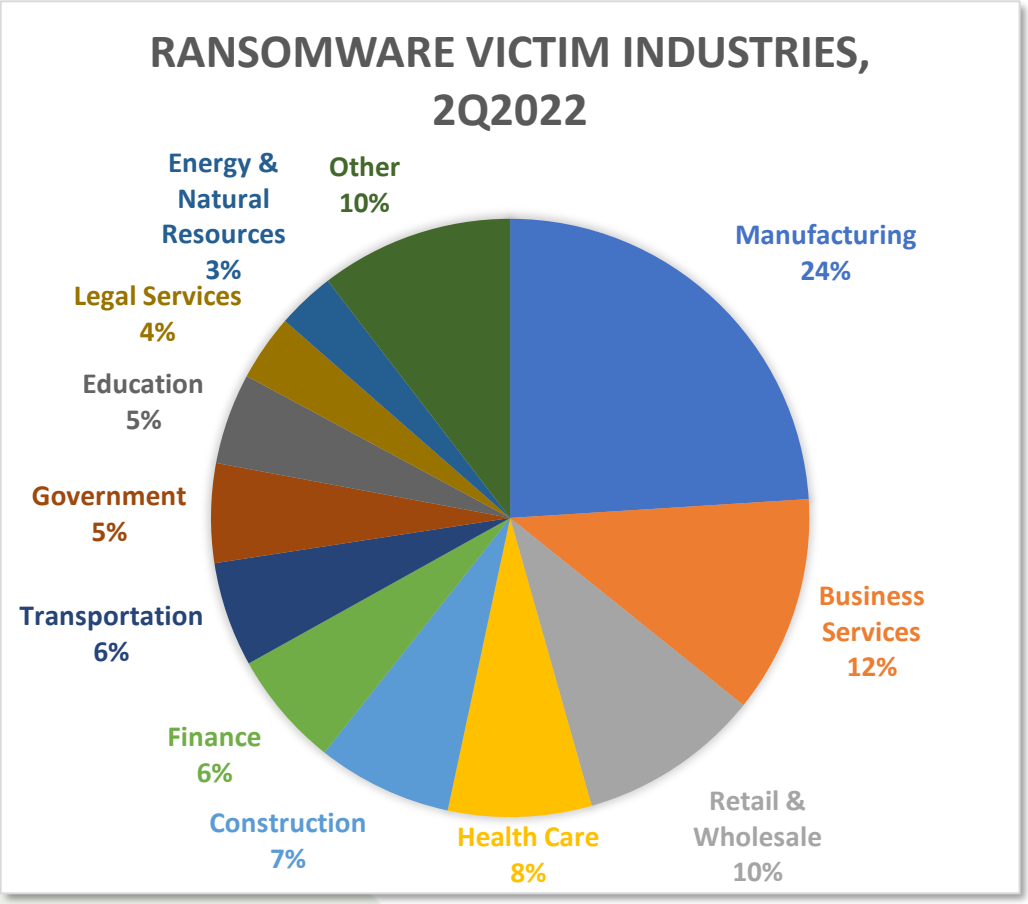
Ransomware – 2nd Quarter 2022

APWG member Abnormal Security tracks ransomware: malware that forces a company to pay a ransom to the perpetrator. The malware may encrypt the victim's data so that it cannot be used until the criminal unlocks it, or it makes the data or system otherwise inaccessible. Abnormal Security tracks and stops ransomware delivered via email to its customers, and tracks victims through a combination of ransomware extortion blog monitoring on the dark web and open-source intelligence collection. These methods provide a representative look at the overall ransomware threat landscape and lets the company make inferences about global ransomware trends.

After spiking in the last quarter of 2021, Abnormal observed a decrease in ransomware volume over the first and second quarters of 2022. In June 2022, Abnormal observed the smallest number of ransomware victim companies since January 2021.



The top industries impacted by ransomware in Q2 2022 were manufacturing, business services, retail and wholesale firms, and the healthcare sector, which includes hospitals:

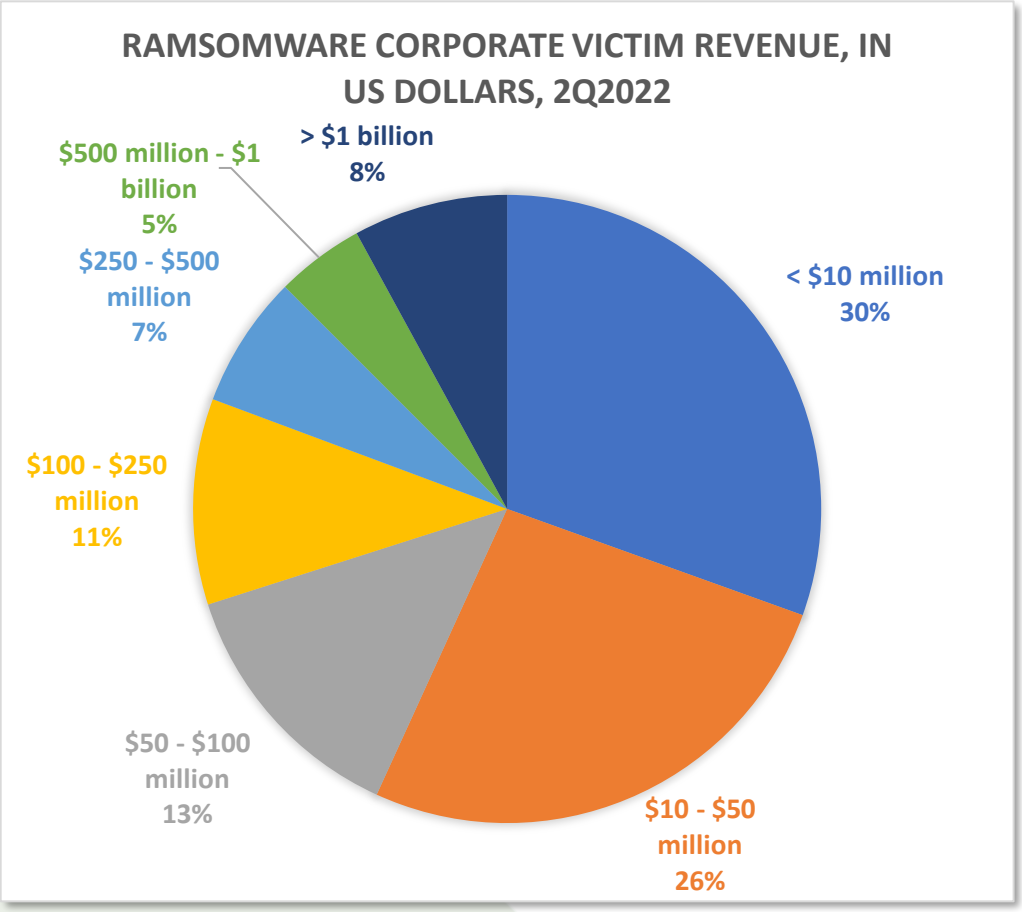


Crane Hassold, Director of Threat Intelligence at Abnormal Security, analyzed the ransomware activity over the quarter. "The Transportation industry saw the largest growth in ransomware victims. Much of the increase in ransomware attacks against transportation companies was due to LockBit's focus on the sector during the quarter. The healthcare industry, which has long been a concerning target of ransomware attacks, also experienced a significant increase in attacks in the second quarter, growing 53 percent compared to the first quarter."

"Almost all global regions saw a net decrease in the number of ransomware victims identified in those regions.," said Hassold. "The one exception was the Asia-Pacific (APAC) region, which saw a 31 percent increase in ransomware victims in the second quarter. Interestingly, the increase of attacks in the APAC region wasn't caused by a spike in activity against companies in a single country. Rather, the number of ransomware victims increased in numerous countries in the region—most notably in Australia, Thailand, Japan, and Taiwan."

About 56 percent of victimized companies had less than US$50 million in revenue, down from about 66 percent in 2021. These smaller companies are generally unable to invest large amounts of money in

cybersecurity, which makes them better opportunistic targets. But almost 13 percent of the victim corporations had deep pockets, with revenues of more than US$500 million:



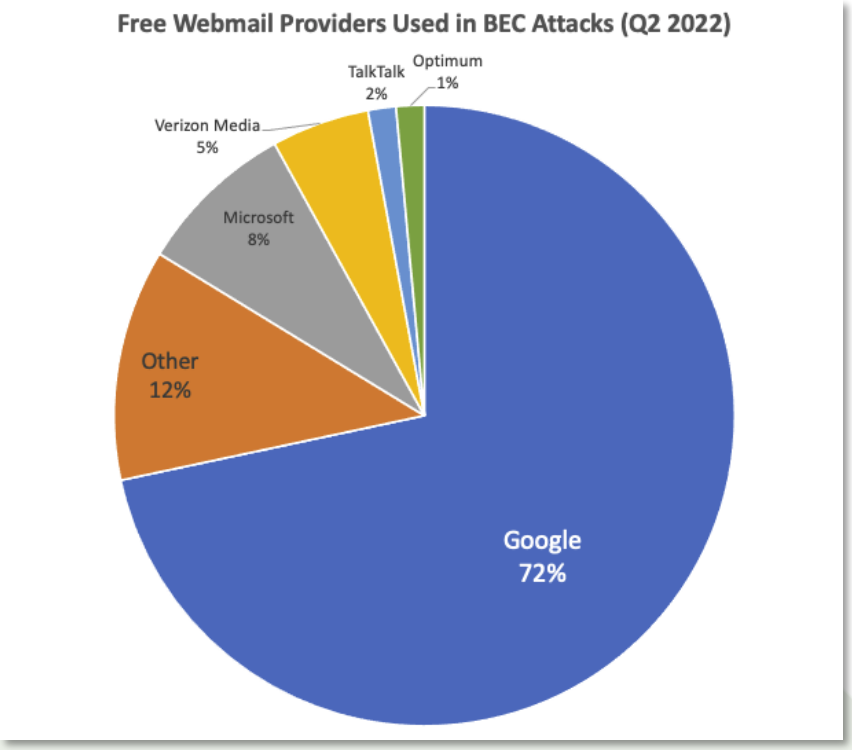
Business e-Mail Compromise (BEC), 1st Quarter 2022

APWG member Agari by HelpSystems tracks the identity theft technique known as "business e-mail compromise" or BEC, which has caused aggregate losses in the billions of dollars, at large and small companies. In a BEC attack, a scammer impersonates a company employee or other trusted party, and tries to trick an employee into sending money, usually by sending the victim email from fake or compromised email accounts (a "spear phishing" attack). Agari examined thousands of BEC attacks attempted during Q2 2022. Agari counts BEC as any response-based spear phishing attack that involves the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive materials. Agari protects organizations against phishing, BEC scams, and other advanced email threats.

In Q2 2022, gift card requests were the most popular cash-out method used by criminals, making up 39.9 percent of the total, followed by payroll diversion attempts (25.9%), advanced fee fraud (15.5%), and wire transfers (9.6%). Agari found that the average amount requested in wire transfer BEC attacks in Q2 2022 was $109,467, up from $91,436 in Q1 2022. A variety of miscellaneous cash out methods accounted for the remaining 9.1 percent.

Q2 2022 saw a jump in gift card requests and a slight increase in wire transfer requests compared to the previous quarter. Google Play was once again the most requested gift card in Q2 2022, accounting for 31.9 percent of all gift card requests. This was followed by Apple's offerings (Apple Store 14.0% + iTunes 8.7%) and Amazon (13.1%). Liquid cards not tied to a specific retailer, such as Mastercard, Visa, American Express, and One Vanilla, made up 17.4 percent of gift card requests.

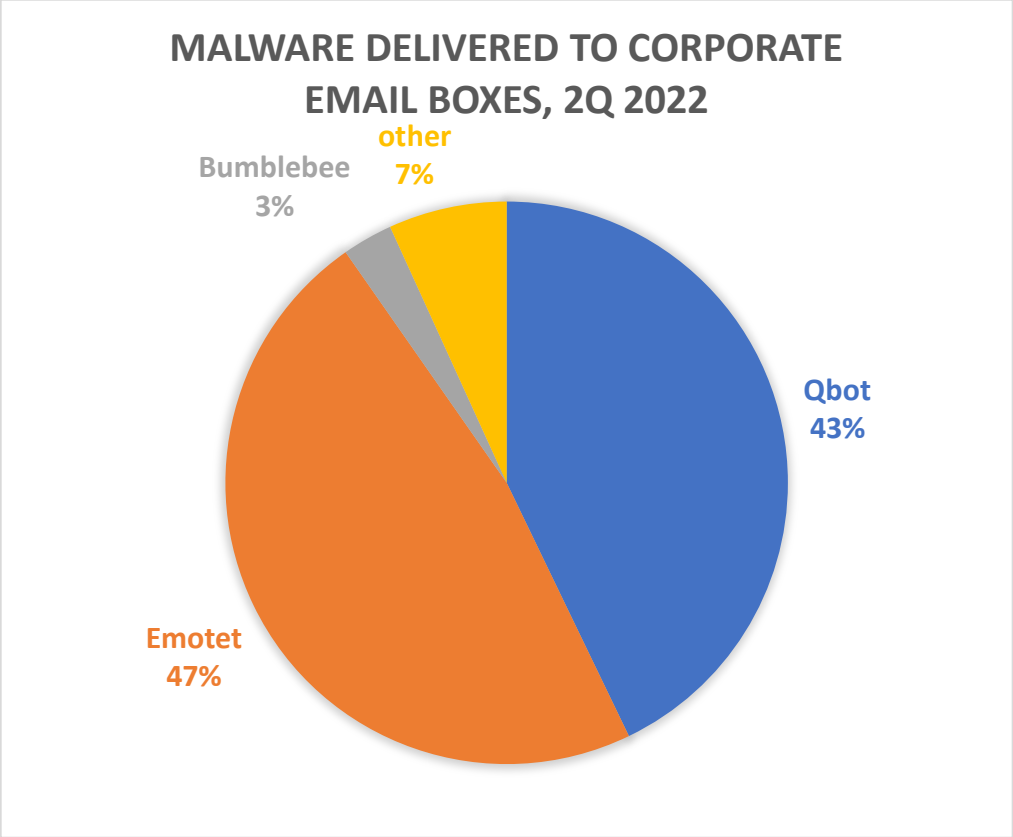
Agari found that 73 percent of BEC attacks in Q2 2022 were launched using a free webmail address. John Wilson, Senior Fellow, Threat Research at HelpSystems, noted that "Google was the single largest technology provider used by BEC criminals, with 72 percent of webmail addresses and 24 percent of maliciously registered domains hosted on Google Gmail email platform." Microsoft (Outlook, Hotmail) was next with 8 percent. followed by Virgin Media at 5 percent.



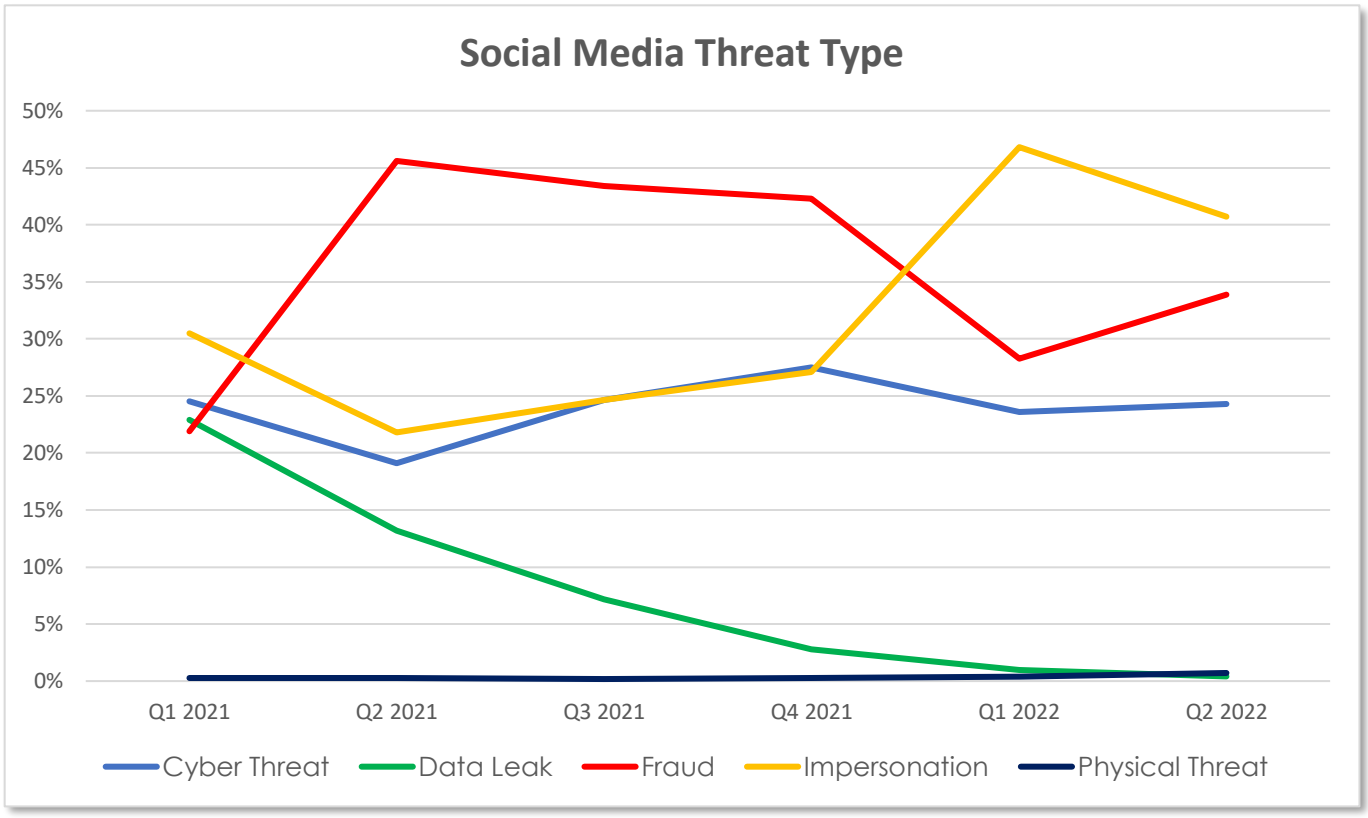
Email-based Threats, 2nd Quarter 2022

[9] APWG member PhishLabs by HelpSystems analyzes malicious emails reported by corporate users.

"The industry is quite good at keeping malware out of enterprise user inboxes," said John Wilson, Senior Fellow, Threat Research at HelpSystems. "However, that's not the case for phishing emails that steal credentials or elicit a response (like BEC). Ninety-five percent of the threats found in enterprise user inboxes in Q2 were either credential theft or response-based attacks."



"Threats on social media continues to rise with a 47 percent increase from Q1 to Q2," said Wilson. "Impersonation and fraud are the top two threats, accounting for three out of every four social media attacks. Malicious actors use social media to reach massive audiences, posing significant risk to enterprises and their brands."


Social Media Threat Type
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
Q1 2021
Q2 2021
Q3 2021
Q4 2021
Q1 2022
Q2 2022
Cyber Threat
Data Leak
Fraud
Impersonation
Physical Threat

APWG Phishing Activity Trends Report Contributors

Abnormal Security provides a leading cloud email security platform to stop attacks that evade traditional Secure Email Gateways.	Agari by HelpSystems protects organizations against phishing, business email compromise (BEC) scams, and other advanced email threats.	Axur works to identify and fight the threats in the cyberspace that interfere with the interests of companies, governments, and individuals.
Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.	OpSec Security offers world-class brand protection solutions.	PhishLabs by HelpSystems provides managed threat intelligence and mitigation services that protect brands, customers, and the enterprise from digital risks.

The *APWG Phishing Activity Trends Report* is published by the APWG. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver (foy@apwg.org, +1.404.434.728). For media inquiries related to the company-content of this report, please contact APWG Secretary General Peter Cassidy (pcassidy@apwg.org, +1.617.669.1123); Anil Prasad at Abnormal Security (www.abnormalsecurity.com/contact), Stefanie Wood Ellis of OpSec Security (sellis@opsecsecurityonline.com); Rachel Woodford of Agari (Rachel.Woodford@helpsystems.com), Eduardo Schultze of Axur (eduardo.schultze@axur.com,+55 51 3012-2987); Rachel Woodford of HelpSystems (Rachel.Woodford@helpsystems.com). **Analysis and editing by Greg Aaron, Illumintel Inc., www.illumintel.com**

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail spoofing. Membership is open to financial institutions, online retailers, ISPs, solutions providers, the law enforcement community, government agencies, multilateral treaty organizations, and NGOs. There are more than 2,200 enterprises worldwide participating in the APWG.

Operationally, the APWG conducts its core missions through: APWG, a US-based 501(c)6 organization; the APWG.EU, the institution's European chapter established in Barcelona in 2013 as a non-profit research foundation incorporated in Spain and managed by an independent board; the STOP. THINK. CONNECT. Messaging Convention, Inc., a US-based non-profit 501(c)3 corporation; and the APWG's applied research secretariat <http://www.ecrimeresearch.org>.

APWG's directors, managers and research fellows advise: national governments; global governance bodies such as the Commonwealth Parliamentary Association, Organisation for Economic Co-operation and Development, International Telecommunications Union and ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe, Europol EC3 and the Organization of American States. APWG is a founding member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations.

APWG eCrimeX

APWG's clearinghouses for cybercrime-related machine event data send more than two billion data elements per month outbound to APWG's members to inform security applications, forensic routines and research programs, helping to protection millions of software clients and devices worldwide. APWG Engineering continues to work with data correspondents worldwide to develop new data resources.

APWG's STOP. THINK. CONNECT. cybersecurity awareness campaign has officially engaged campaign curators from 26 nations, 13 of which are deployed by cabinet-level ministries, government CERTs and national-scope NGOs.

STOP|THINK|CONNECT MESSAGING CONVENTION

The annual APWG Symposium on Electronic Crime Research, proceedings of which are published by the IEEE, attracts scores of papers from leading scientific investigators worldwide. The conference, founded in 2006 by APWG, is the only peer-reviewed conference dedicated exclusively to cybercrime studies.

eCrime2022 Symposium on Electronic Crime Research