

FORTRA[®]

2024 Brand Threats and Fraud Report

Introduction

In the second quarter of 2024, Fortra analyzed hundreds of thousands of domains, social media, counterfeit, and dark web attacks targeting enterprises, their employees, and brands. This report uses the data from those attacks to present key trends shaping the threat landscape. Security leaders and practitioners can use this information to better understand these threats and to take proactive measures to reduce risk.

Key Findings

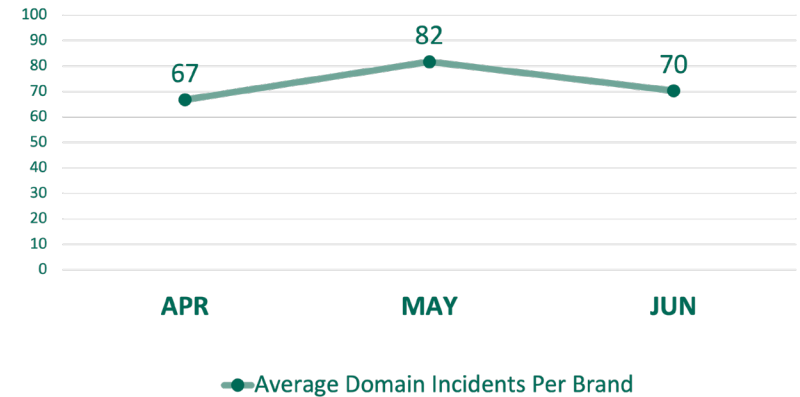
- ▲ The use of New Generic Top-Level Domains (New gTLD) to create phishing sites experienced the highest growth in usage by threat actors, surpassing Legacy gTLDs and Country Code TLDs in growth for Q2 2024.
- ▲ The average number of social media attacks per brand increased over 60% quarter over quarter.
- ▲ The average number of counterfeit sites developed to attack enterprises increased 55% quarter over quarter in Q2.
- ▲ While stolen credit card data continued to be most prevalent on the Dark Web, the presence of Fraud Tools and malicious services for hire increased by nearly 21% in Q2.

Domain Impersonation



Look-Alike Domains Per Brand

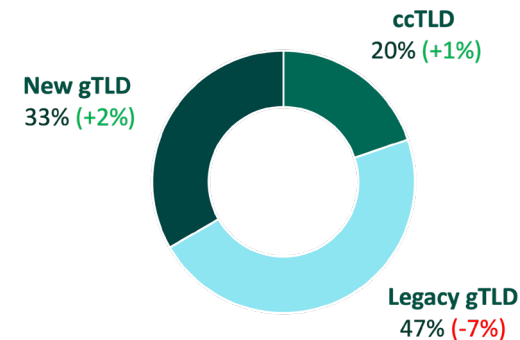
In Q2, Fortra observed an increase in the number of average look-alike domains per brand from Q1, with a peak of monthly activity in May 2024 exceeding 80 attacks per brand. While fluctuations occurred throughout the quarter, enterprises experienced a concerning average of 73 look-alike domain attacks per month.



Top-Level Domain Abuse

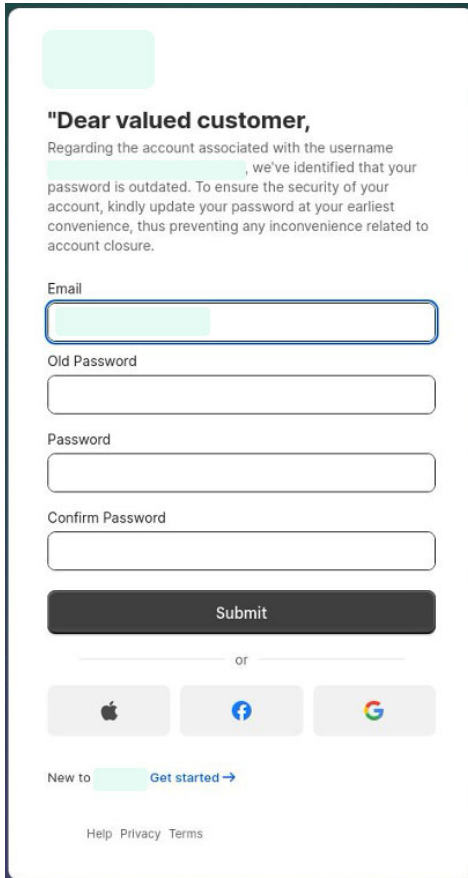
Nearly 47% of all phishing sites observed in Q2 were staged using Legacy Generic Top-Level Domains (Legacy gTLD), such as .com, .org, and .net. This is despite a 7% decline in shared abuse. In fact, the data trends demonstrate that gTLDs have declined in growth for three consecutive quarters. Among gTLDs, .com continued to represent the most Top-Level Domain abuse, contributing to almost 40% of the total volume. This activity was followed by an increase in New gTLD activity across the board, led by a sharp uptick in malicious activity utilizing .dev, and smaller but noticeable increases in activity around .vip, and Russia's .ru country code TLD.

TLD	% PHISH	+/-
.com	36%	-8%
.dev	12%	+11%
.vip	5%	+3%
.ru	5%	+3%
.org	5%	+3%
.info	3%	-2%
.net	3%	+2%
.top	2%	-4%
.online	2%	-1%
.app	2%	0%
Q1 to Q2 2024 Top 10 TLDs that Dropped		
.xyz	0.4%	-1.94%
.life	0.3%	-1.35%
.io	0.6%	-1.09%



TLDs such as .xyz, .life, and .io experienced the largest decline in attack volume of Top-Level Domain Abuse. The trend demonstrates an average decline of approximately 1.5%, with a small volume of incidents that make up a combined 0.4% of all Top-Level Domain Abuse threats.

Recent Threats Using New .dev and .vip Top-Level Domains (TLDs)



"Dear valued customer,
Regarding the account associated with the username [redacted], we've identified that your password is outdated. To ensure the security of your account, kindly update your password at your earliest convenience, thus preventing any inconvenience related to account closure.

Email
[redacted]

Old Password
[redacted]

Password
[redacted]

Confirm Password
[redacted]

Submit

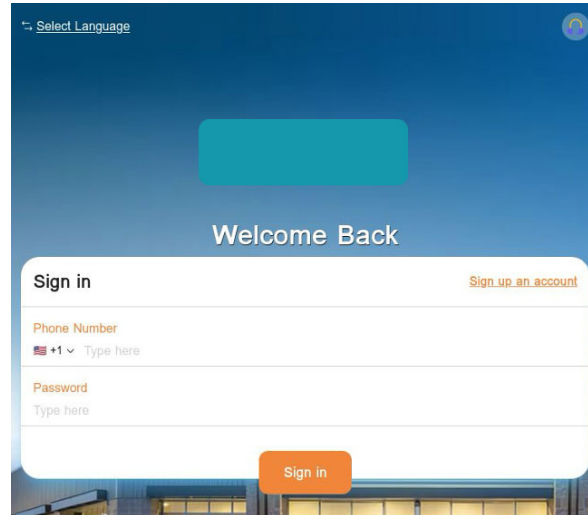
or

Apple Facebook Google

New to [redacted] [Get started →](#)

[Help](#) [Privacy](#) [Terms](#)

[brandname]-support.pages.dev



Select Language

Welcome Back

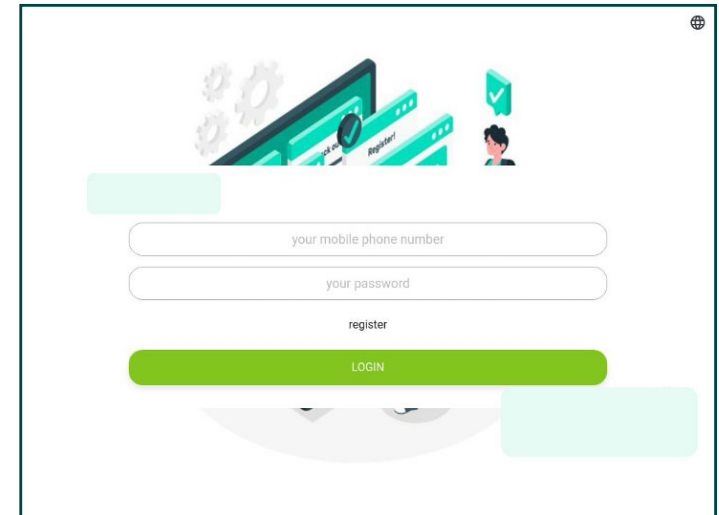
Sign in [Sign up an account](#)

Phone Number
+1 Type here

Password
Type here

Sign in

jw-ab-[brandname].pages.dev



your mobile phone number

your password

register

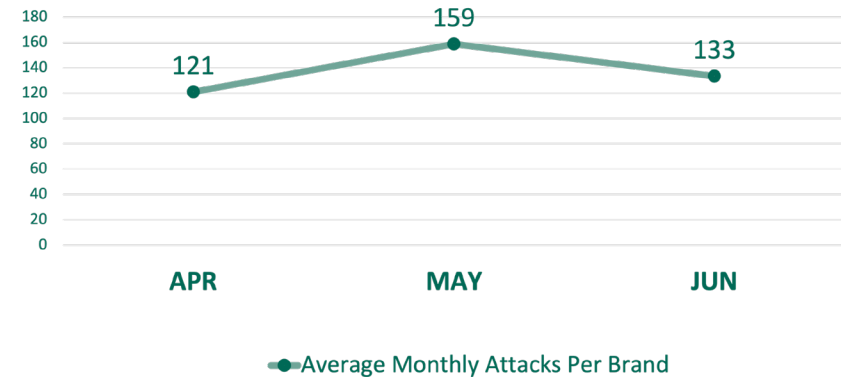
LOGIN

www.8[brandname].88.vip

Social Media

Social Media Attacks Per Brand

In Q2, enterprises experienced an average of 138 social media attacks per month. Early Q2 experienced the lowest number of attacks at 121. However, attacks surged to almost 160 attacks per month in May alone, representing a concerning 27% increase from the start of the quarter. When performing the same comparison quarter over quarter, the increase in attack volume is even larger at over 60%.



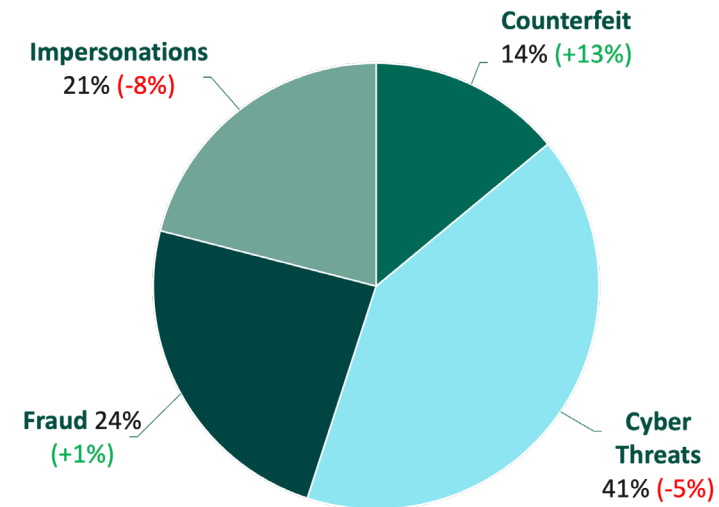
Top Social Media Threat Types

Although Counterfeits make up 14% of all social media threats in Q2, they experienced the highest growth in attacks compared to other categories. Counterfeit instances grew by 13% in Q2, a significant contrast to the combined decline of 4% observed across all social media threat types.

Fraud threats, such as the exposure of banking details and banking fraud, were the next highest growing social media threat type in Q2, increasing modestly by 1% in Q1 and accounting for 24% of all social media threats.

Impersonations, including the spoofing of corporate brands, executives, and employees, declined 8% in Q2. In fact, these attacks have consistently decreased in activity since Q4 2023.

Cyber Threats, such as hacking, decreased 5% in Q2, but continued to remain the top social media threat type experienced by organizations.



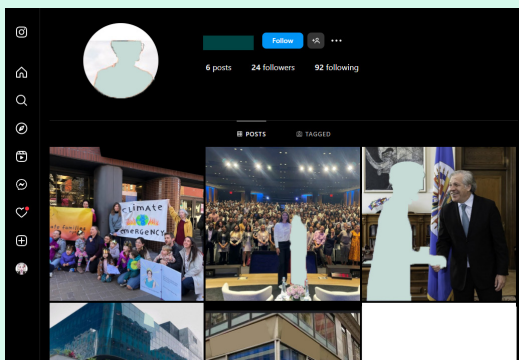
Note: Percent change compares data from Q1 2024 – Q2 2024.

Top Social Media Threat Types (Continued)

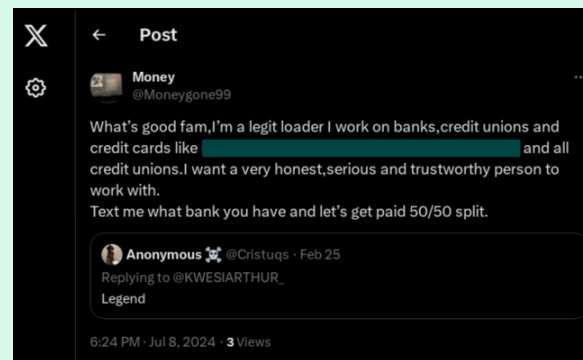
Below are the definitions of the various Social Media Threat Types as defined by Fortra:

- **Fraud:** An incident designed to deceptively deny a right to a victim or provide illegal gain to the threat actor, including the unauthorized sale of account credentials, exposure of banking details such as BIN numbers, deposit fraud, providing access to tools designed to commit fraud, and other financial threats.
- **Impersonation:** The spoof of a corporate brand, executive, or employee with intent to sway opinion or fool victims into performing an action.
- **Cyber Threat:** An incident that includes an intentional cyber risk to the targeted victim, such as hacking attempts.
- **Counterfeits:** Incidents with the intent to create or distribute fake versions of products, websites, items, software, and other digital assets. These threats tend to mimic legitimate brands and aim to steal sensitive data, spread malware, or commit fraudulent activities.

Recent Social Media Threat Examples



EXECUTIVE IMPERSONATION



DEPOSIT FRAUD

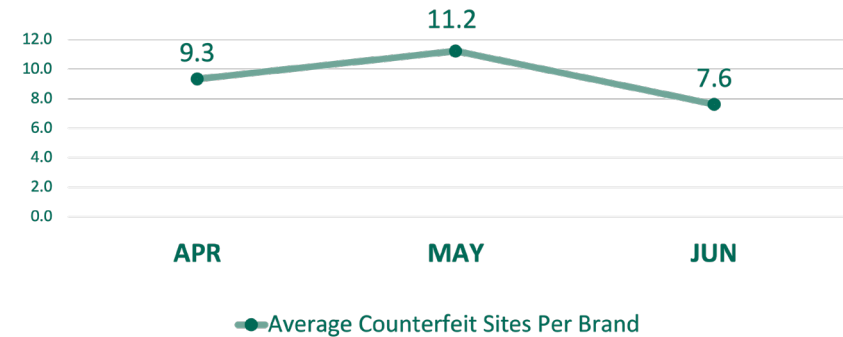


LEAKED DATA

Counterfeit Sites

Counterfeit Sites Per Brand

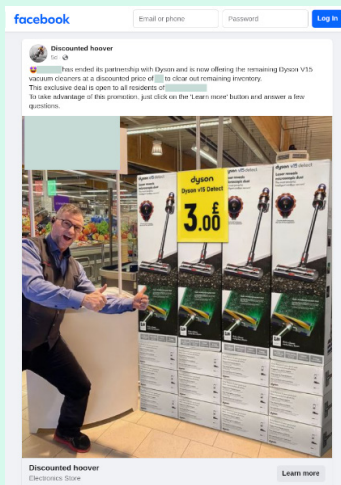
In Q2, the average number of counterfeit sites that attacked enterprises increased more than 50% from Q1 2024. Attacks peaked in May, at just over an average of over 11 per brand, which is an 18% increase compared to April. On average, brands experienced a startling 55% increase in counterfeit threats compared to the previous quarter.



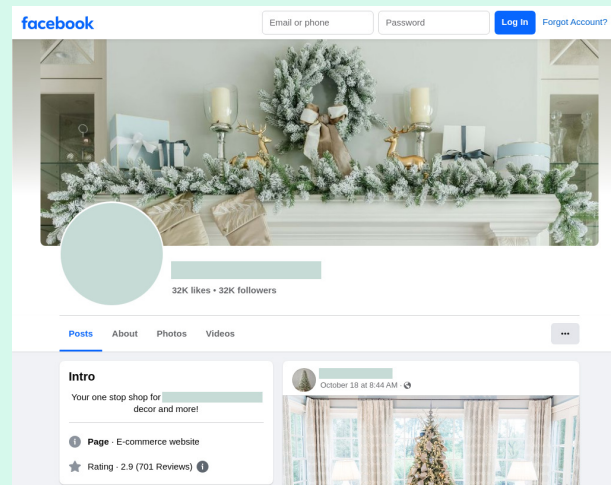
Note: Brands used in these calculations include organizations whose services and industries are naturally prone to counterfeit threats.

Counterfeit Threat Examples

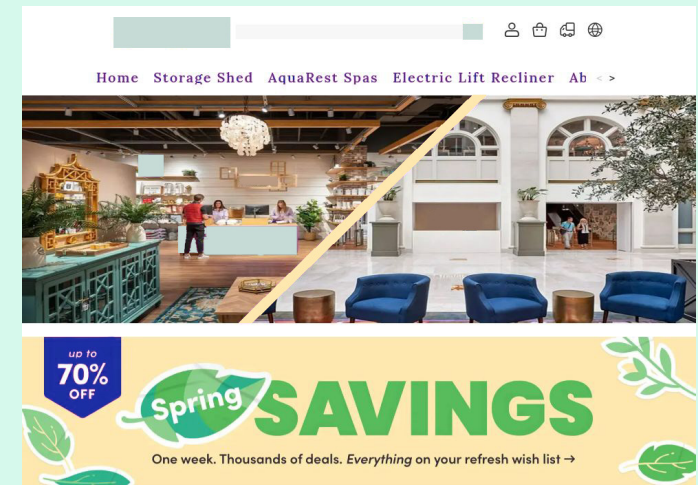
The following are examples of counterfeit attacks, a type of threat that often starts with a social media advertisement designed to lure users to a malicious social media page or counterfeit e-commerce site. These threats impersonate popular brands through the usage of logos, branding styles, and look-alike domains that attempt to trick the user into purchasing and interacting with counterfeit items.



Social Media Ad



Social Media Page



Counterfeit E-Commerce Site

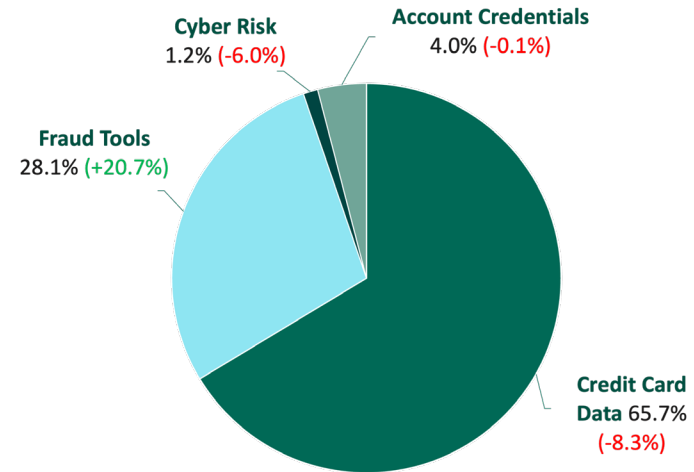
Dark Web

Top Dark Web Threats

Credit Card Data and Fraud Tools contributed to 93.8% of all threats on the dark web. Although stolen and remarketed Credit Card Data decreased by 8.3% compared to the previous quarter, it continued to make up nearly 70% of the detected threats plaguing organizations in Q2.

Most notably, the growth of Fraud Tools, designed to compromise corporate environments, more than doubled compared to last quarter, positioning it as the highest growing threat for enterprises on the dark web in Q2.

Account Credentials contributed to 4% of the total volume of dark web threats, and Cyber Risk made up the smallest amount of dark web threats at 1.2%.

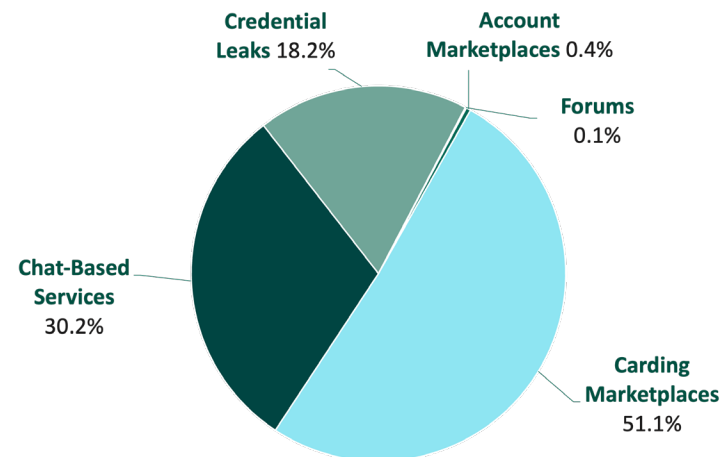


Top Dark Web Site Types

In Q2, stolen data on the dark web was most frequently marketed in Carding Marketplaces specializing in the sale of account and card data. In fact, over half of the dark web sites used to market and share stolen data were Carding Marketplaces.

The use of Chat-Based Services as an advertising platform accounted for just over 30% of observed dark web activity, while Credential Leaks accounted for an additional 18.2% of observed threats.

Account Marketplaces, dedicated primarily to selling account-based data, and Forums rounded out the top five, contributing a small amount for Q2 and adding up to less than a percent of the overall dark web activity recorded for the quarter.



Recent Dark Web Brand Threats

Fraud » Verified Accounts

[REDACTED] | Full Access [PREMIER SERVICE]

xiao_baobei Rating: 4.9 out of 5 Reviews: 786 Sales: 12949

250 USD

1

* Bitcoin and Monero accepted

Description Reviews

Comes with:

- ✓ Mail Access
- ✓ Fullz/SSN that was Used
- ✓ Bank Account Login
- ✓ Cookies
- ✓ Secret Answers

ACCOUNT CREDENTIALS FOR SALE

Other » Guides and Tutorials

i WILL TEACH YOU How to card [REDACTED] tutorial

TrioGram Rating: 5 out of 5 Reviews: 48 Sales: 62

36 USD

1

* Bitcoin and Monero accepted

Description Reviews

i WILL TEACH YOU How to card [REDACTED] tutorial

Carding [REDACTED] is easy if you have the right tools, follow the right method and use the right fire cc from [REDACTED]

Before we proceed on this tutorial, I would like to explain what [REDACTED] for the interest of those who might [REDACTED]

You can send without installing the app on your phone, though you can download [REDACTED] and connect [REDACTED] make sure it is with your primary account.

[REDACTED]

bank. The growing list of participating banks includes titans such as [REDACTED]

FRAUD TOOLS

Seller	Base	CVR	BIN	EXP	Info	zip	State	City	Country	Price
seller17296	[24.10.2023] American cards HQ PT3	72%		04/2027					United States	8.50 \$

STOLEN CARD DATA

Conclusion

In the second quarter of 2024, Fortra identified multiple brand threat and fraud trends across digital channels:

Domain impersonation attacks followed an upward trend for the year throughout the second quarter of 2024, with a 20% surge in attacks occurring within a single month. On average, organizations can expect 73 domains per month that maliciously mimic their own. The rise in these attacks can expose organizations to multiple risks including damages to brand reputation, loss of consumer trust, and financial losses.

Phishing remains one of the most prevalent threats affecting organizations, their employees, and clients. Nearly half of all the phishing sites in Q2 were staged using Legacy Generic Top-Level Domains (Legacy gTLDs). Among the Top-Level Domains (TLDs) exploited in Q2, .com and .dev accounted for most phishing sites observed, comprising 48% of all TLD abuse.

Social media attacks increased 60% quarter over quarter. This trend highlights the speed and ease at which threat actors can target brands with malicious campaigns on social channels, emphasizing the need for detection and monitoring capabilities across popular platforms. The vast user base, constant flow of information, and the shift of younger generations relying more on social platforms for information instead of web searches create the ideal environment for cyber threats. As of Q2, the average organization experienced nearly 138 attacks per month on social channels.

Counterfeit threats have also surged, with elevated levels of attacks persisting throughout the quarter. In Q2, counterfeit sites and posts increased by more than 50% compared to Q1. These sites often impersonate well-known technology and retail brands to lure customers into engaging with knockoffs and can introduce security vulnerabilities as they may contain malicious elements that can further increase the attack surface area.

The significant rise in online brand threats and fraud highlights the need for continuous vigilance and adaptation. As threat actors continue to refine and shift their tactics, organizations must prioritize threat intelligence, robust defense strategies, and cyber vigilance to maintain resiliency against these evolving threats and risks.



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.