CSC® DIGITAL BRAND SERVICES
CORPORATION SERVICE COMPANY®

CYBER SECURITY REPORT

January 2017

Research and editorial prepared by CSC® Digital Brand Services

This CSC Digital Brand Services Quarterly Cyber Security Report culls all the most important information about cyber crime and cyber security for you in one comprehensive version—giving you the most up-to-date information in one place for you to quickly scan the news that's important to you and your brand.

In this first edition, our experts present the most recent intelligence focused around domain name systems, distributed denial of service attacks, phishing and email fraud, and domain security.

Christopher Ross,
global brand analyst

Hari Reddy,
product manager, brand protection services

Mark Flegg,
global product director of domains and security

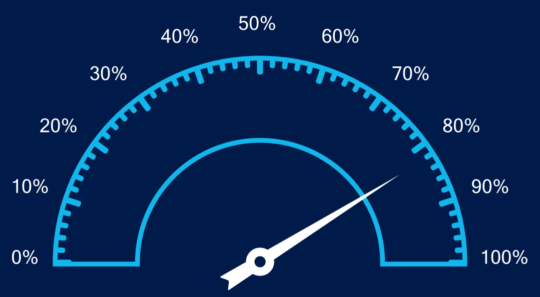
Vincent D'Angelo,
director, Brand Advisory Team

Marie Le Maitre,
global marketing manager

The Domain Name System and Distributed Denial of Service Attacks

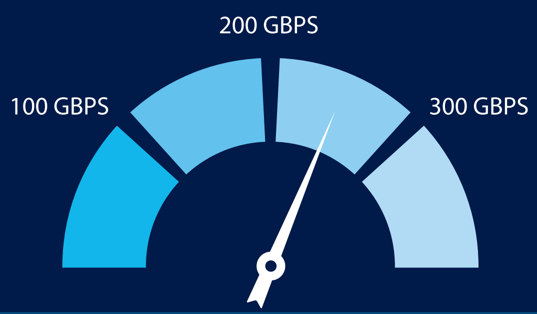
The Domain Name System (DNS) is a frequent target for cybercriminals, and the most common DNS threat is a Distributed Denial of Service (DDoS) attack. Cyber crime is becoming more sophisticated by the day—and the Internet of Things has become an unwilling partner in this crime.

Attack frequency:



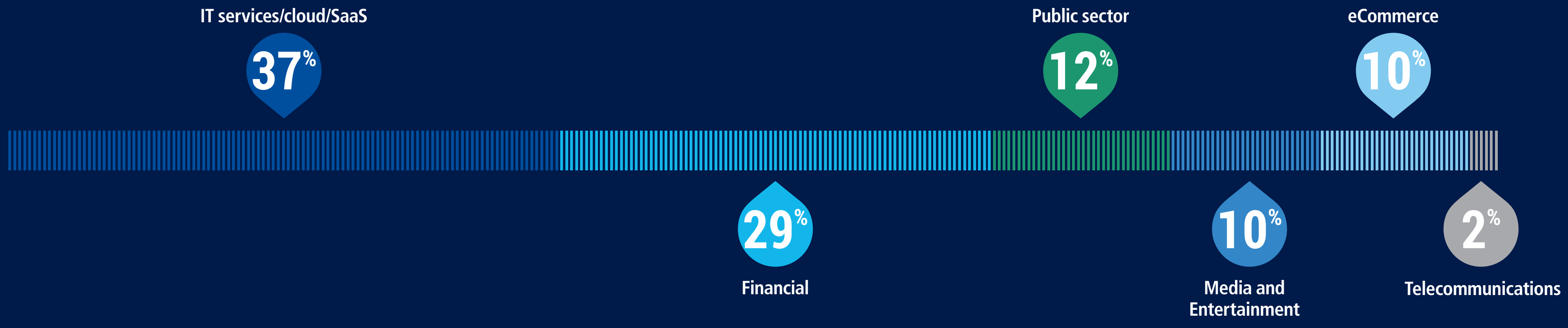
- Average peak attack size increased **82%** since Q3 2015; overall the average peak attack sizes in Q3 2016 have been larger than previous recorded years.
- Also, **41%** of customers in Q3 2016 were attacked multiple times.

Attack size:



- The largest volumetric attack in Q3 2016 observed directly by Verisign® peaked at **257 Gbps**. However, others in the industry observed much larger attacks of, for example, **620 Gbps**, which was launched against **KrebsOnSecurity.com**.
- IT Services, the financial industry, as well as the public sector, continue to experience some of the largest attack sizes in Q3 2016.

Mitigations on behalf of Verisign customers by industry for Q3 2016:



SOURCE: *Verisign Distributed Denial of Service Trends Report, Volume 3, Issue 3 – 3rd Quarter 2016: "DDoS Attacks Become More Sophisticated and Persistent."*

Every organization is at risk: *Examples in the news*

Even KrebsOnSecurity.com gets hacked

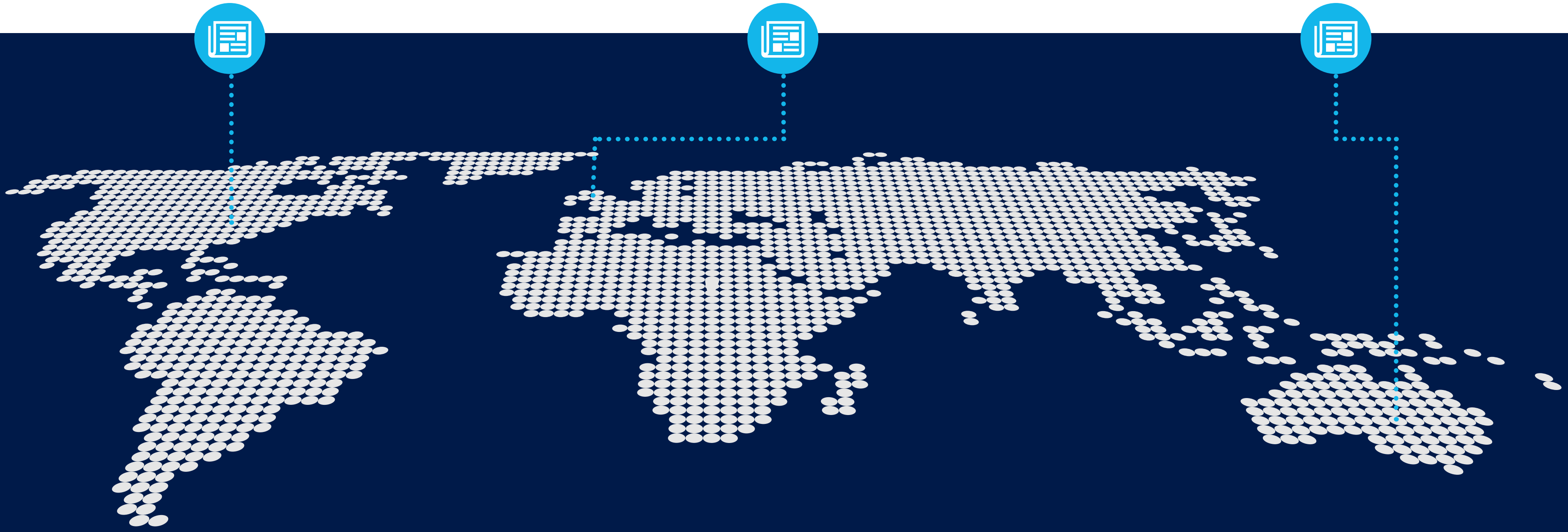
In September 2016, a record-breaking 620 Gbps DDoS attack—one of the largest in 2016—was directed at Brian Krebs, an American cyber crime investigative journalist. It appeared to be launched by a huge botnet of hacked Internet of Things devices. The mitigation provider for Krebs eventually surrendered to the attack, and his site went black.

1, 2, 3—attack!

123-Reg admitted they fell victim to a "huge scale" DDoS attack in summer 2016. The website hosting provider was hit with an attack of over 30 Gbps. And even though their protection services mitigated some of the attack, customers still experienced connection issues—and for a few customers, data was even entirely lost—so it was no surprise that customers took their frustrations to social media.

Australian census kicked offline

Being attributed to overseas hackers, the Australian Bureau of Statistics website crashed on August 9, 2016 during their first-ever digital census. Australian's—required to complete a census every five years—were keen to try the new system with officials saying two thirds of citizens were slated to use the online system. Investigators say the attack was clearly malicious.



Growing trend

Courtesy of **Verisign**

Low-volume application layer, also known as Layer 7 attacks, probe for vulnerabilities in application code, employing various techniques to use HTTP/S field headers within request packets in order to disable the application. These attacks are frequently coupled with high volume User Datagram Protocol flood attacks to distract the victim from the Layer 7 attack component.

These types of sophisticated low-bandwidth DDoS attacks are a form of denial of service attack that typically uses less traffic but increases its effectiveness by aiming at a weak point in the victim's system design.

These attacks often utilize structured query language (SQL) injection, a code injection technique, to attack data-driven applications by inserting nefarious SQL statements into the request entry fields for execution. The malicious requests typically include long "Host:" values in the request.

Layer 7 attacks often require multiple and advanced filtering techniques, including adaptive origin response code and regex based filtering, along with network protection techniques like SYN authentication, invalid IP fragments, and UDP flood filtering.

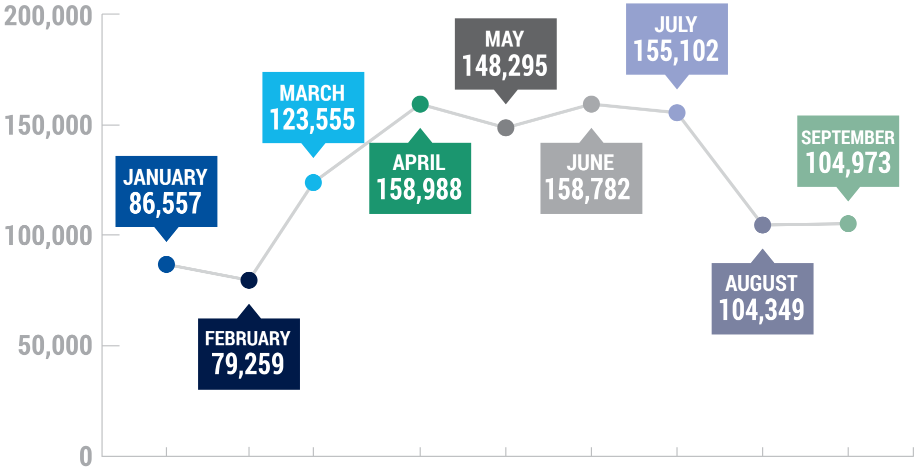
For all the information on the growing trend, **read the Verisign report**.

Phishing and Email Fraud

Phishing could be considered the biggest threat to business security worldwide. It remains an all-too-common vehicle for corporate data breaches, credit card fraud, and identity theft, with phishing scams getting more innovative and costly every year.

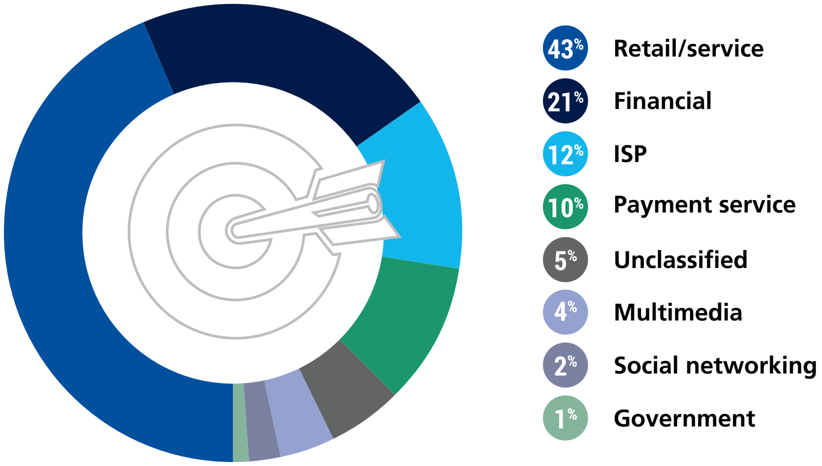
Unique phishing sites observed:

The total number of phishing sites observed in **Q3 was 364,424**, compared with **466,065 in Q2, showing a decline of 25%**. The total number of phishing sites observed in Q2 of 2016, however, was an all-time high.



Most targeted industry sectors:

The retail and service sector remained the most targeted during the third quarter of 2016, suffering **43%** of attacks.



Phishers targeted **between 340 and 361** unique brands a month in Q3. This is slightly fewer than in Q2, when **between 411 and 425** brands were attacked each month. This **17% drop** coincides with generally lower numbers of phishing attacks.

SOURCE: *APWG Phishing Activity Trends Report, 3rd Quarter 2016. Most targeted industry sectors statistics are from Q2 2015.*

Every organization is at risk:

Examples in the news

CEO fired after $42M cyber fraud

A hoax email in May 2016 where cyber criminals posed as the company's CEO—also known as spear phishing—is what led to the theft of €50M euros and the immediate dismissal of Walter Stephan, CEO of FACC, an Austrian aerospace parts manufacturing company. The "fake president incident" convinced an employee to wire money to the criminals for a fake acquisition. FACC was able to block €10.9M euros from being transferred, but they suffered an operating loss of €23.4M euros—over five times that of their previous year's losses.

Gumtree.com.au hijacked for malvertising

In March 2016, online ads on gumtree.com.au led clickers to ransomware—the Angler Exploit kit—that stole bank credentials. Simply clicking the link could compromise the user's computer. Cyber criminals hacked the account used by a legitimate Australian law firm to place the ads, posing as the law firm itself, even using its logo. The hackers created a sub-domain of the law firm's domain, and even alternated between legitimate ads and ransomware ads to keep the scam from being detected.

Dell defaced

A hacker who goes by "MuhmadEmad" from KurdLinux_Team—a Kurdish hacking group—defaced Dell's official site after gaining access to the website's subdomains in the summer of 2016. The reason appeared to be political, but it wasn't clear at the time why Dell was chosen to be hacked and defaced. MuhmadEmad posted a message on Dell's website and even posted a video about exactly how he did it.

The Rio Olympics of spamming

The popularity of the Olympic Games in Rio attracted the attention of scammers and spammers starting in 2015. From fake notifications of lottery winnings, to unsolicited advertisements, and goods and services promising to make the consumer an Olympian, the scams took advantage of the theme and likeness of the Games to swindle people into buying fake tickets, and giving the fraudsters access to people's bank accounts. Scammers even went as far as registering websites complete with SSL certificates to make legitimate looking, protected websites with HTTPS URLs, all the better to fool consumers with.

Not even grocery stores are safe

Employee financial information was compromised at the Sprouts Farmers Market in April 2016. The result: fraudulent credit cards were opened in employee's names, and even their tax refunds were stolen right out from under them. The data breach affected over 20,000 people and all started with a phishing scam that gave the criminals access to employee W2s, allowing them to file fraudulent tax returns in employees' names.

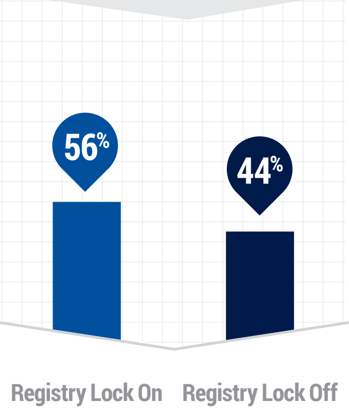
Domain Security

We looked at the domain security of 50 well-known global brands to assess their cyber security risk. We observed their main domain names and analyzed their security posture based on what we deem to be critical aspects in this ecosystem. The following statistics show that there's still a great deal of work to be done getting companies up to speed on domain security, and our teams are working with clients daily to get them secure.

REGISTRY LOCK

RISK

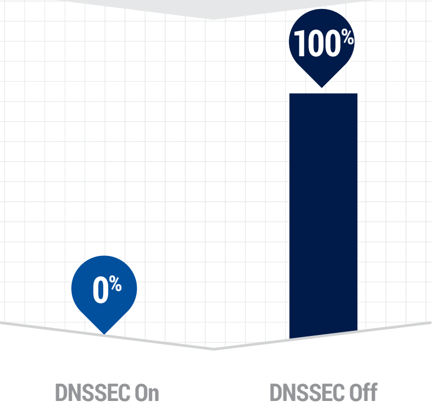
Unlocked domains are vulnerable to social engineering tactics leading to unauthorized DNS changes.



DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

RISK

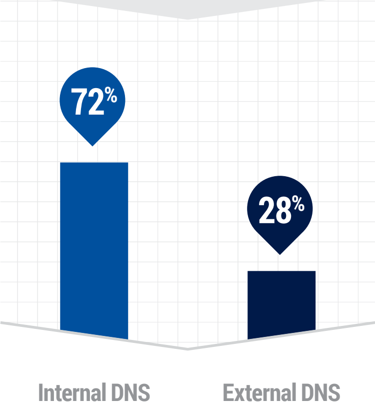
Lack of deployment leads to vulnerabilities in the DNS which includes an attacker hijacking any step of the DNS lookup process. As a result, hackers can take over control of a session and redirect users to their own deceptive websites.



DNS PROVIDER (INTERNAL VS. EXTERNAL)

RISK

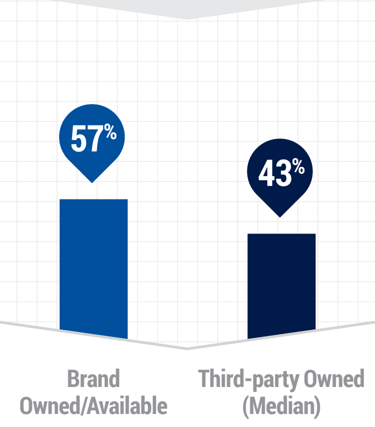
Non-enterprise level DNS providers pose potential security threats like DDoS attacks, as well as downtime and revenue loss.



THIRD-PARTY OWNED TYPOS

RISK

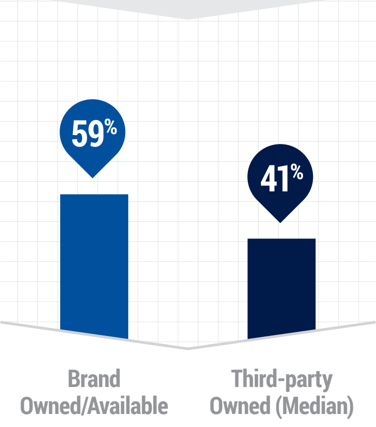
Typos can be used as malicious vectors to divert consumers to fraudulent third-party websites that phish for information or distribute malware.



THIRD-PARTY OWNED TYPOS WITH MAIL EXCHANGER RECORDS

RISK

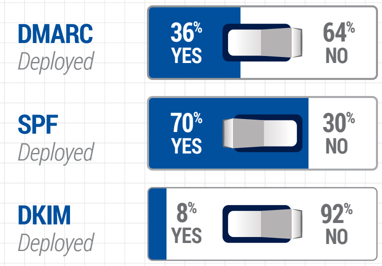
Email typos can be used as malicious vectors for phishing and to intercept email traffic.



EMAIL AUTHENTICATION

RISK

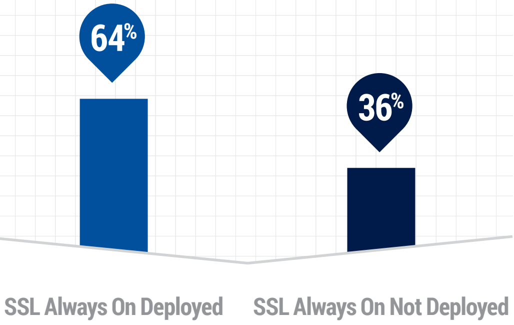
Authenticating the email channel with Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF), or DomainKeys Identified Mail (DKIM) minimizes the incidence of email spoofing and potential phishing.



SECURE SOCKETS LAYER (SSL) ALWAYS ON

RISK

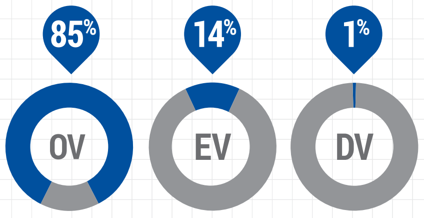
Safe encryption for all online transactional business that mitigates the security risk of cyber criminals hijacking web sessions in order to commit identity theft or install malware on user devices, or hackers infringing on web communications that could lead to a breach, theft of customer data, a DDoS attack, or defacing a website.



SSL TYPE (EV, DV, OR OV)

RISK

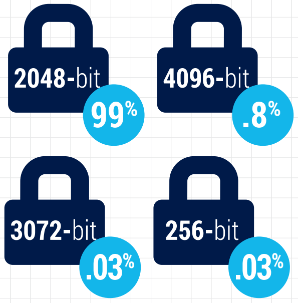
SSL types that require more authentication, such as organization validation (OV) and extended validation (EV) are less prone to compromise rather than domain validation (DV).



ENCRYPTION LEVEL

RISK

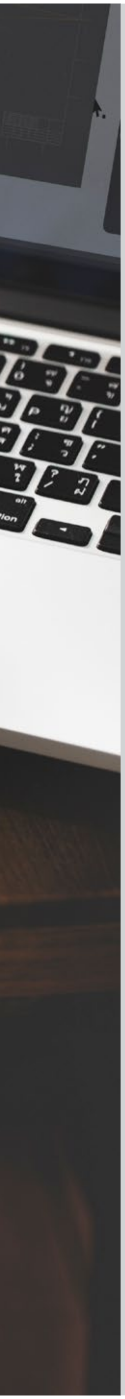
SSL types that have higher encryption are less prone to compromise.



CSC DIGITAL BRAND SERVICES
CORPORATION SERVICE COMPANY

Cyber Security Report

Observation Trends AMONG 50 WELL-KNOWN GLOBAL BRANDS



CORPORATE REGISTRAR UTILIZATION

70%

A majority of large brand owners (70%) utilize a corporate registrar to manage their main domain name as opposed to a retail corporate registrar.
cscdigitalbrand.services/blog/think-a-retail-registrar-is-the-way-to-go-think-again/

REGISTRY LOCK UTILIZATION

56%

A little more than half of large brand owners are utilizing Registry Lock.
cscdigitalbrand.services/blog/no-access-allowed/

GLOBAL BRANDS NOT RELYING ON OUTSOURCED ENTERPRISE CLASS DNS SOLUTIONS

72%

Due to the magnitude of DDoS attacks, it is surprising that many global brands (close to three quarters) are not relying on outsourced enterprise class DNS solutions.
cscdigitalbrand.services/blog/cyber-attacks-do-you-have-a-response-plan/

DOMAIN AND EMAIL TYPOS WHICH CAN BE USED AS PHISHING AND MALWARE

40%+

It is concerning that more than 40% of possible domain and email typos are owned by third parties which can be used as phishing and malware vectors.

DNNSEC DEPLOYMENT

0%

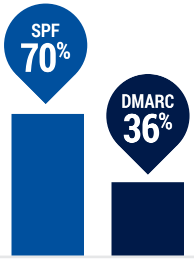
Because of negligible adoption globally, no brands have deployed DNNSEC.

TOP BRAND DOMAINS NOT USING ALWAYS-ON SSL

36%

Websites with no SSL encryption are being flagged by Google® as unsecure and not safe—and as a result are falling in the organic rankings. So, it's quite interesting that 36% of top brand domains still do not deploy always-on SSL.

MOST USED EMAIL AUTHENTICATION PROTOCOLS

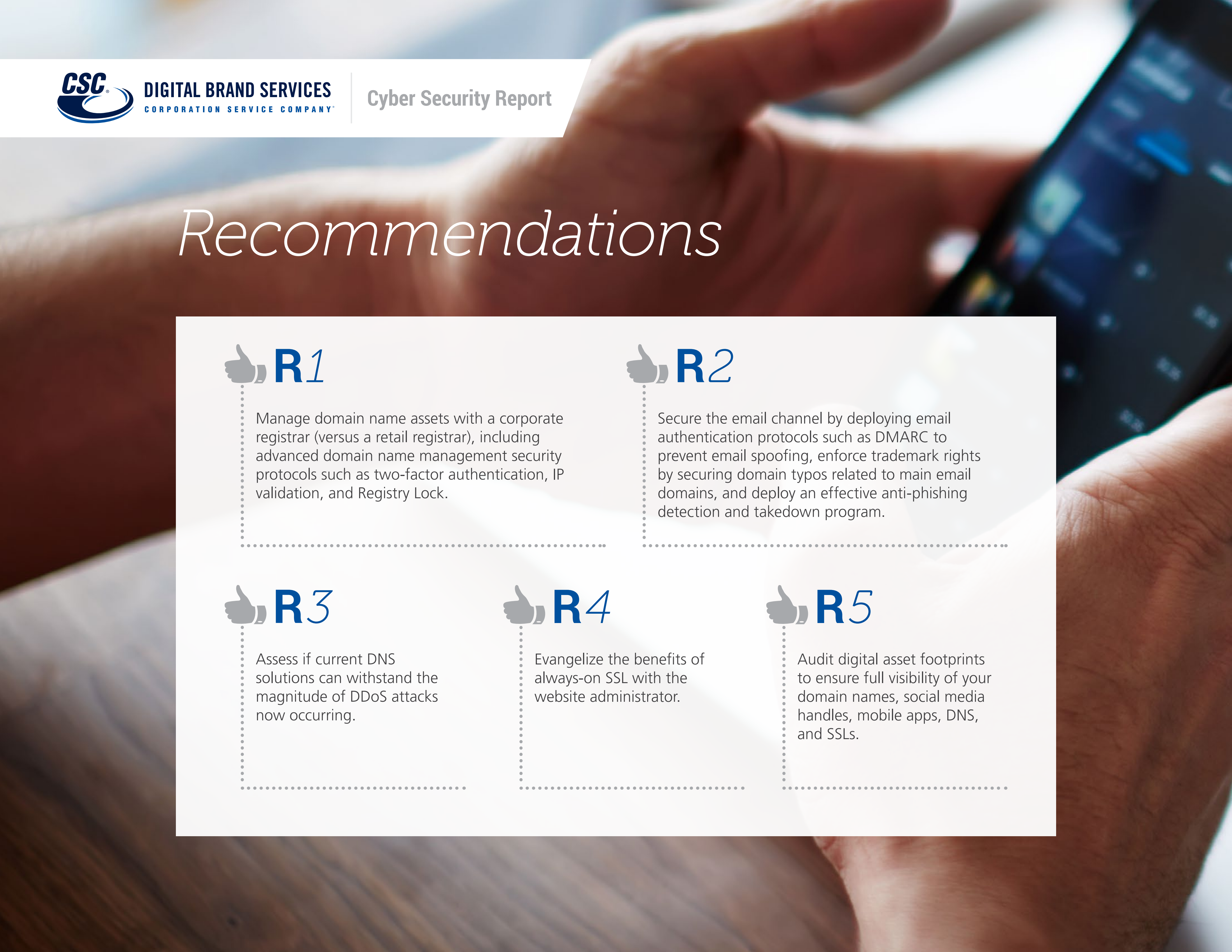


In terms of authenticating the email channel, DMARC (36% adoption) and SPF (70% adoption) are the most used protocols. However, it is concerning that 100% adoption of DMARC isn't yet deployed as this can effectively reduce phishing. In addition, Google and Microsoft® are securing the email channel with DMARC which may block your customers from receiving your emails.

TOP BRAND DOMAINS WITH OV SSLs DEPLOYED

85%

It comes as no surprise that 85% of top brands have deployed OV SSLs with 99% of SSLs having 2048-bit encryption.



Recommendations

R1

Manage domain name assets with a corporate registrar (versus a retail registrar), including advanced domain name management security protocols such as two-factor authentication, IP validation, and Registry Lock.

R2

Secure the email channel by deploying email authentication protocols such as DMARC to prevent email spoofing, enforce trademark rights by securing domain typos related to main email domains, and deploy an effective anti-phishing detection and takedown program.

R3

Assess if current DNS solutions can withstand the magnitude of DDoS attacks now occurring.

R4

Evangelize the benefits of always-on SSL with the website administrator.

R5

Audit digital asset footprints to ensure full visibility of your domain names, social media handles, mobile apps, DNS, and SSLs.

CONSOLIDATE *AND* **SECURE** *YOUR DIGITAL ASSETS*

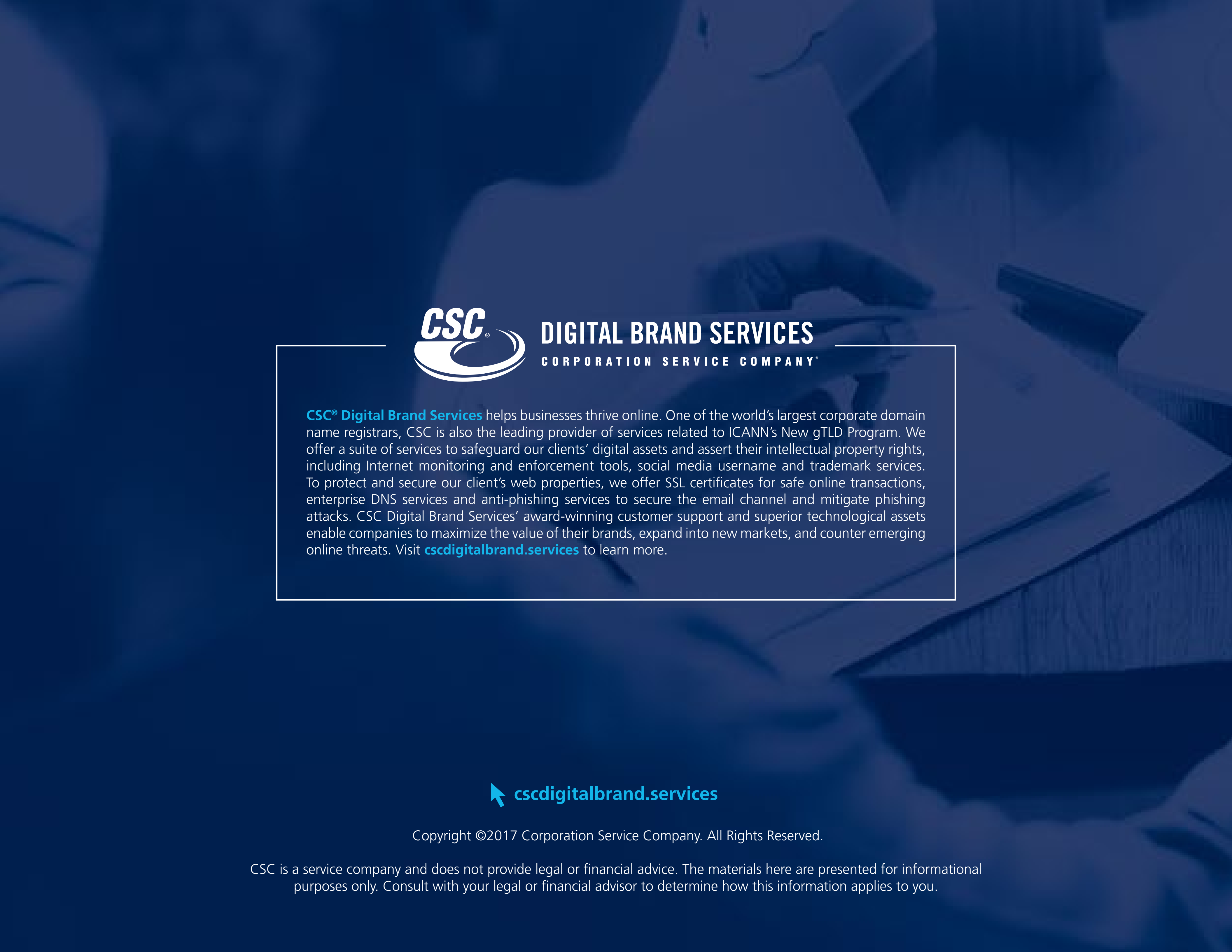
Centralizing your digital assets puts you in control. CSC Digital Brand Services helps you manage your domain names, social media usernames, SSL, and DNS more efficiently to secure them against cyber attacks.

OPTIMIZE *AND* **PROMOTE** *YOUR DIGITAL PORTFOLIO*

Developing a connected digital brand strategy ensures your digital portfolio is working hard. CSC helps you find the optimum mix of assets—including .brands—to drive traffic and support your campaigns while minimizing online brand abuse.

MONITOR *FOR THREATS AND* **ENFORCE** *YOUR RIGHTS*

Protecting your brands online means detecting and removing threats. CSC Digital Brand Services helps you monitor your brand across the digital channels, prioritize results, and take action against the most serious infringements.



CSC® DIGITAL BRAND SERVICES

CORPORATION SERVICE COMPANY®

CSC® Digital Brand Services helps businesses thrive online. One of the world's largest corporate domain name registrars, CSC is also the leading provider of services related to ICANN's New gTLD Program. We offer a suite of services to safeguard our clients' digital assets and assert their intellectual property rights, including Internet monitoring and enforcement tools, social media username and trademark services. To protect and secure our client's web properties, we offer SSL certificates for safe online transactions, enterprise DNS services and anti-phishing services to secure the email channel and mitigate phishing attacks. CSC Digital Brand Services' award-winning customer support and superior technological assets enable companies to maximize the value of their brands, expand into new markets, and counter emerging online threats. Visit **cscdigitalbrand.services** to learn more.

cscdigitalbrand.services

CSC is a service company and does not provide legal or financial advice. The materials here are presented for informational purposes only. Consult with your legal or financial advisor to determine how this information applies to you.