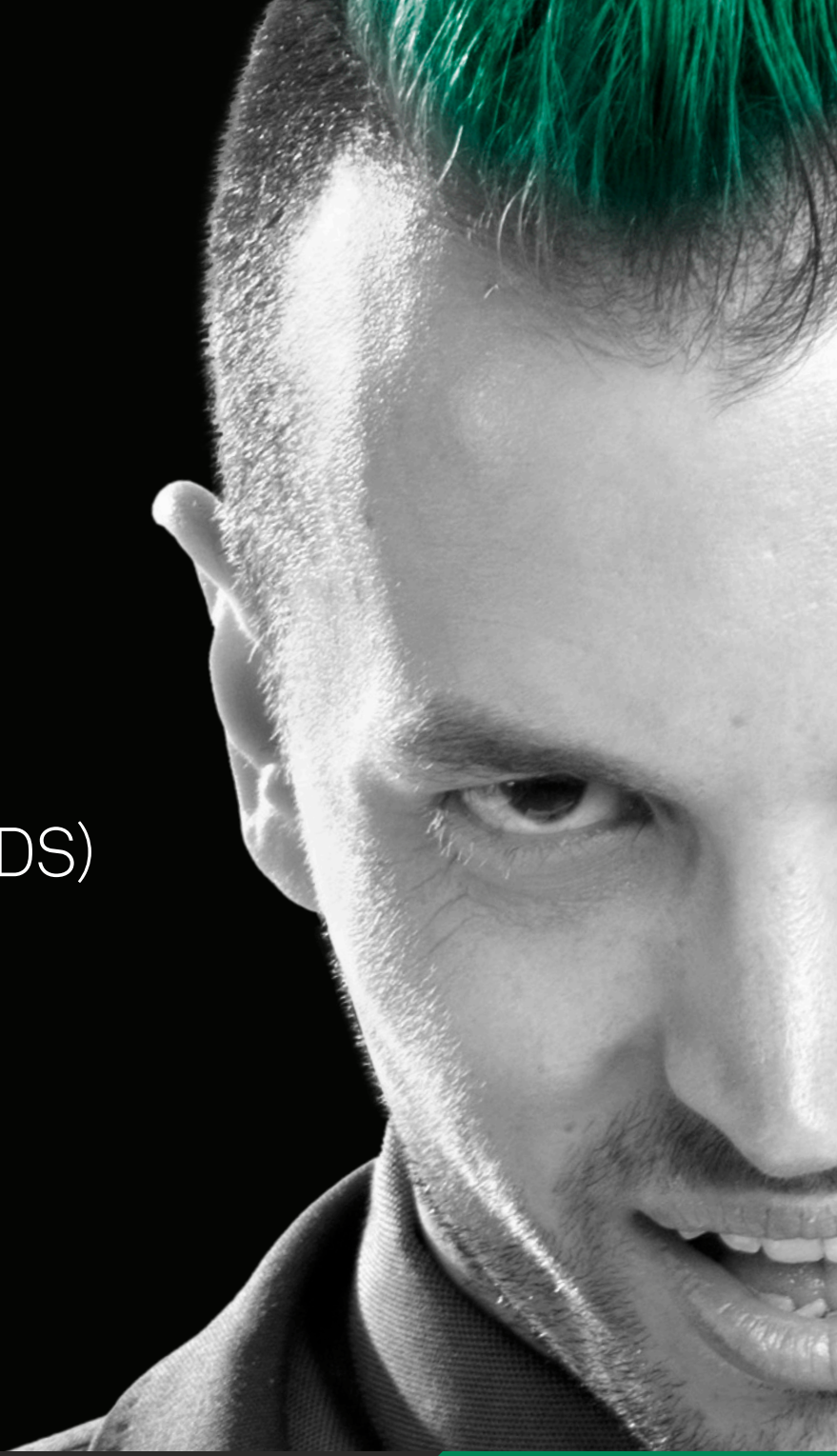
6 THREATS TO HOLIDAY WEBSITE SHOPPING

(AND 2 SELF-INFLICTED WOUNDS)



neustar

THERE ARE THREATS TO ONLINE SHOPPING EVERY DAY OF THE YEAR.

THE HOLIDAYS, OF COURSE, SIMPLY MAGNIFY THE RISKS.

During Q4 the financial stakes become stratospheric:

$100B

in holiday online spend

In 2014, according to Digiday

$480K

per hour in Cyber Monday losses

From DDoS and other cyber-attacks, as reported by RSA Security and the Ponemon Institute

"SMART CARDS"

expected to drive more fraudsters online

Credit cards that store data in chips, not magnetic stripes, reduce in-store fraud. Look for fraudsters to migrate to your website.

THE BUYING PATH IS STREWN WITH THREATS.

SOMETIMES THE ENEMY IS YOU.

Read on...
to see each threat from the attacker's point of view, along with counter-measures to minimize their impact.

We'll begin at the beginning, when someone types your URL, follow the journey through your site, and finish with post-sale outreach.

neustar

DNS ATTACKS

Customers try to reach your site, but get hijacked to bogus pages.

DDOS ATTACKS

Where'd your website go?

FAILURE TO LOAD TEST SITE/MONITOR PERFORMANCE

Site crashes under peak traffic or pages/ applications run slowly.

SLOW PAGES AND APPLICATIONS

Site underperforms. Are you monitoring and testing rigorously?

REGISTRATION/ AUTHENTICATION FRAUD

Fraudsters login with stolen credentials.

TCPA VIOLATIONS

Whether you're making special offers or collecting debts, non-compliant auto-dialing can mean big fines.

PAYMENT/ TRANSACTION FRAUD

Criminals make fraudulent purchases with stolen credit card data.

PHISHING ATTACK

Scammers forge emails to lure your customers to unsafe pages. Just what you need as your marketing team is doing post-sale upsells.

neustar

DNS ATTACKS

“I can stop the gift-giving before it even begins.”

MOTIVES:

- Steal your customers’ credentials
- Steal their credit card data
- Sell customer data in the cyber-underground or commit fraud themselves
- Disgruntled customer gets revenge by making your site unavailable

Through cache poisoning, aka DNS spoofing, attackers can trick a recursive nameserver into returning a wrong IP address to an end-user. That would be *their* address, a bogus site where they siphon off logins, passwords, and credit card numbers. Attackers can accomplish the very same thing by hacking into and changing your DNS records, often at the domain registrar.

Alternatively, to crash your site on Cyber Monday, an attacker could launch a DNS reflection attack. He/she would send spoofed DNS queries, crafted to generate huge responses, to open recursive servers. Some of the largest DDoS attacks in the past two years have done just this.

neustar

DNS ATTACKS

COUNTER-MEASURES:

- DNSSEC (DNS security extensions)—Digital signatures ensure that DNS responses are identical to those from your authoritative server. Protect against forged or manipulated data.
- Managed DNS service with hardened security features—The best third-party DNS providers include DNS protection at no extra cost. Non-open source resolvers (unlike BIND) are less prone to malware, viruses, and attacks. Purpose-built DDoS protection—Hybrid solutions are best, combining on-premises hardware and cloud-based protection. See the following section for more details.
- Give your DNS the advanced security: permission levels, two-factor authentication, and access control list (ACL) by IP to restrict access to DNS records.

neustar

DDOS ATTACKS

"No site, no online holiday sales."

MOTIVES:

- Take you offline and demand ransom
- Competitor seeking an edge
- Political/social activism
- Smokescreen malware or virus insertion

Powered by cheap attack tools that are openly sold online, DDoS is maybe the easiest way to disable your holiday website. As described in the previous section, DNS is one of many attack vectors. To knock you offline, attackers have plenty of other tactics.

Volumetric Attacks—The idea is to saturate the target site's bandwidth with high-volume traffic. Attacks of this type include UDP floods, ICMP floods, and other spoofed-packet floods.

Protocol Attacks—These attacks consume server resources, or those of related communication equipment, like firewalls and load balancers. Some examples: SYN floods, fragmented packet attacks, Ping of Death, and Smurf DDoS.

Application Layer Attacks—Often masked as legitimate traffic, these more surgical attacks aim to crash the web server. Common types: Slowloris, zero-day attacks, Windows or open BSD vulnerabilities, and attacks that target Apache.

COUNTER-MEASURES:

Purpose-built DDoS protection such as...

- On-premises hardware
- Cloud-based traffic scrubbing
- A hybrid of both

88%
OF CONSUMERS DISTRUST
websites that crash

Source: Neustar, "What Erodes Trust in Digital brands?" July 2015

neustar

FAILURE TO LOAD TEST SITE/ CLOSELY MONITOR PERFORMANCE

“What do you mean our server just crashed on Cyber Monday?”

THE GOOD NEWS:

Your website gets more traffic during Q4.

THE BAD NEWS:

If you don’t test your site to handle peak traffic, disaster lurks. You could suffer a self-inflicted wound.

SOLUTION:

It’s more like a pre-measure.
Load test early.
Be prepared.

Load testing ecommerce sites is a pre-holiday must. By bombarding your site with traffic in a controlled environment, you can gauge capacity under heavy loads, discover performance gaps leading to slow page loads, and have the time to remediate the most urgent problems.

Testing lets you know how your site will likely perform on Black Friday, Cyber Monday, or a Wednesday in early December. Well in advance of the holiday crush, you can tackle common issues like bandwidth limitations, error rates exceeding thresholds, and server PU limitations.

neustar

REGISTRATION/AUTHENTICATION FRAUD

"Am I really Debbie from Cleveland? Yeah, sure I am…"

MOTIVES:

- Use someone else's identity to make online purchases.
- The Internet combines anonymity, reach, and speed. What more could a criminal want?
- As the holidays get rolling, there's an uptick in activities like registering on shopping sites and applying online for credit. You need to confirm on the spot whether a request is legitimate or based on stolen or fictitious identities.
- Quickly and accurately validate Debbie's information—and make sure she's really not Donnie from Kalamazoo.

REGISTRATION/AUTHENTICATION FRAUD

COUNTER-MEASURES:

- Cross-check name, address, phone number, email and IP address
- When validating credit or account applications, identify if a person or bot has completed the form
- Verify, validate, and standardize every new address on applications
- Append alternate contact information on new applications
- Understand phone attributes that are characteristic of fraud; separate VoIP from standard landlines
- Identify recently active or highly inactive phones
- Identify prepaid wireless phones

neustar

TRANSACTIONAL FRAUD

"My billing address says Dallas, but my IP address says Kiev."

MOTIVES:

- Use stolen credit card data to make fraudulent purchases
- Because physical credit cards are becoming more secure, thanks to chip-based smart technologies, thieves are expected to commit more "card-not-present fraud," using credit card data stolen elsewhere to plunder shopping sites.
- Online fraudsters take advantage of anonymizing proxy servers, which hide their IP addresses. When successful, fraudsters fleece innocent consumers and increase your operating costs. According to banktech.com, card-not-present fraud will increase from $3.3 billion to $6.4 billion by 2018, a jump of 106%.

neustar

TRANSACTIONAL FRAUD

COUNTER-MEASURES:

IP data solutions work in real time to help you balance security with customer convenience. So do third-party data identification solutions, used heavily by banks to detect fraud in online applications.

- To ensure a "not present" card belongs to the person using it, cross-check address to phone number
- Examine phone attributes that are commonly associated with fraud: pre-paid, discontinued, VoIP
- Verify email address
- Verify ship-to addresses when different from billing address
- Use IP intelligence to know where and how your consumers connect to the web
- Compare your consumers' IP location with their billing addresses
- Create geolocation-based rules to dictate automatic actions that block or flag suspicious transactions
- Use an IP reputation system to score addresses for fraud risk
- Analyze IP network data to show anonymizing proxy servers

neustar

PHISHING SCAMS

"Dear valued 'customer,' have we got a deal for you!"

MOTIVES:

- Steal your customers' credentials
- Steal their credit card data
- Sell customer data in the cyber-underground or commit fraud themselves

After making a purchase on your website, your marketing team will follow-up with cross-sell or up-sell offers. Many of these will be sent in emails. Certain emails, however, won't really come from your business but from phishing scammers.

Every day, millions of phishing emails arrive in consumers' inboxes. They look perfectly authentic, just like any from your company. When someone clicks, they either unwittingly activate malware or find themselves on a criminal's site, which again easily passes for the real thing. Some malware tracks your keystrokes, which can exposure your passwords across numerous systems, resulting in massive exposure.

Anyone who logs into a phishing site gets their credentials nabbed. Anyone who enters credit card data is ripe for future fraud.

neustar

PHISHING SCAMS

COUNTER-MEASURES:

- Use SPF, DKIM and DMARC records in DNS
- Validate email via DNS records and enforce policy in the event of an authentication failure
- Consider a third party anti-phishing service, such as Agari, which can minimize the chances of phishing emails reaching your customers and abusing your domain name
- Purchase the various TLD versions of your domain and have them redirect to your main website (example.tv → example.com)
- Purchase look-a-like domains so they cannot be exploited by hackers (exemple.com → example.com)

neustar

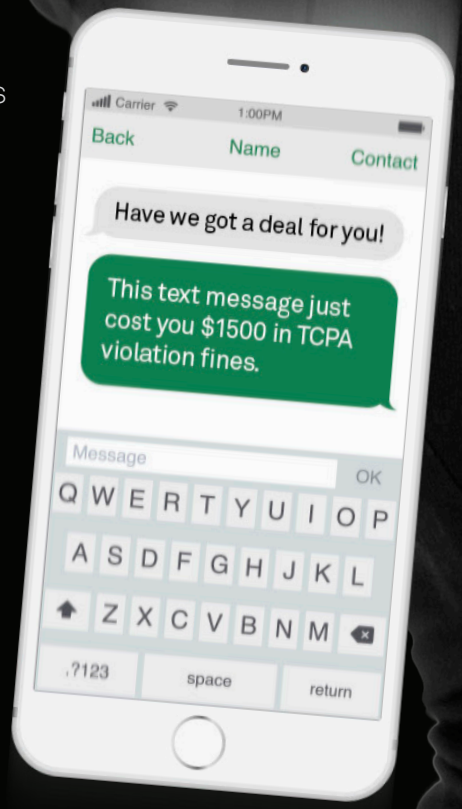
TCPA VIOLATIONS

"Hi, this is Phil calling John Smith with a special offer. You are John Smith, right?"

Your marketing department or call center may auto-dial or text consumers, recent customers and prospects which could be in violation of the Telephone Consumer Protection Act (TCPA). TCPA compliance requires that companies obtain consumer consent and verify that a phone has not been reassigned before auto-dialing or texting any phone number. Identifying incorrect contact information can be challenging as phone numbers are constantly being reassigned to new consumers.

Failure to adhere to TCPA regulations can result in expensive litigation and regulatory actions. Companies that contact consumers directly via unsolicited calls or texts have become the target of class action lawsuits, resulting in steep fines collectively costing those organizations hundreds of millions of dollars.

It's a serious quandary: do you return to manual dialing and kill operational efficiency or continue dialing automatically and risk legal penalties?



SOLUTION:

Make sure your consumer data is constantly updated, so you can reduce TCPA risks AND raise efficiency by increasing right-party contacts; the right vendor can deliver on both.

OVER
2300
TCPA LAWSUITS
in 2014 alone

Source: WebRecon, LLC

#1
CONSUMER COMPLAINT TO FCC
Unwanted telemarketing calls and texts

Source: WebRecon, LLC

neustar

"WHY DO I ROB BANKS? THAT'S WHERE THE MONEY IS."

Willie Sutton, Depression-era gangster

If Slick Willie were alive today, he'd put down his Tommy Gun and fire up his laptop. The Internet is where the money is; during the holidays it gushes. While theft is only one motive for ruining your year-end, it combines with others to threaten to your business and deprive you of sleep. If you see pitfalls in your customers' path to online purchase, take action sooner than later.

Neustar is here to help with:

- Managed DNS
- DDoS protection
- Website performance management (load testing and site monitoring)
- Fraud prevention
- TCPA Risk Mitigation Solutions

neustar

ABOUT NEUSTAR

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time.

More information is available at
http://www.neustar.biz

EB-SEC-1050 09022015

neustar