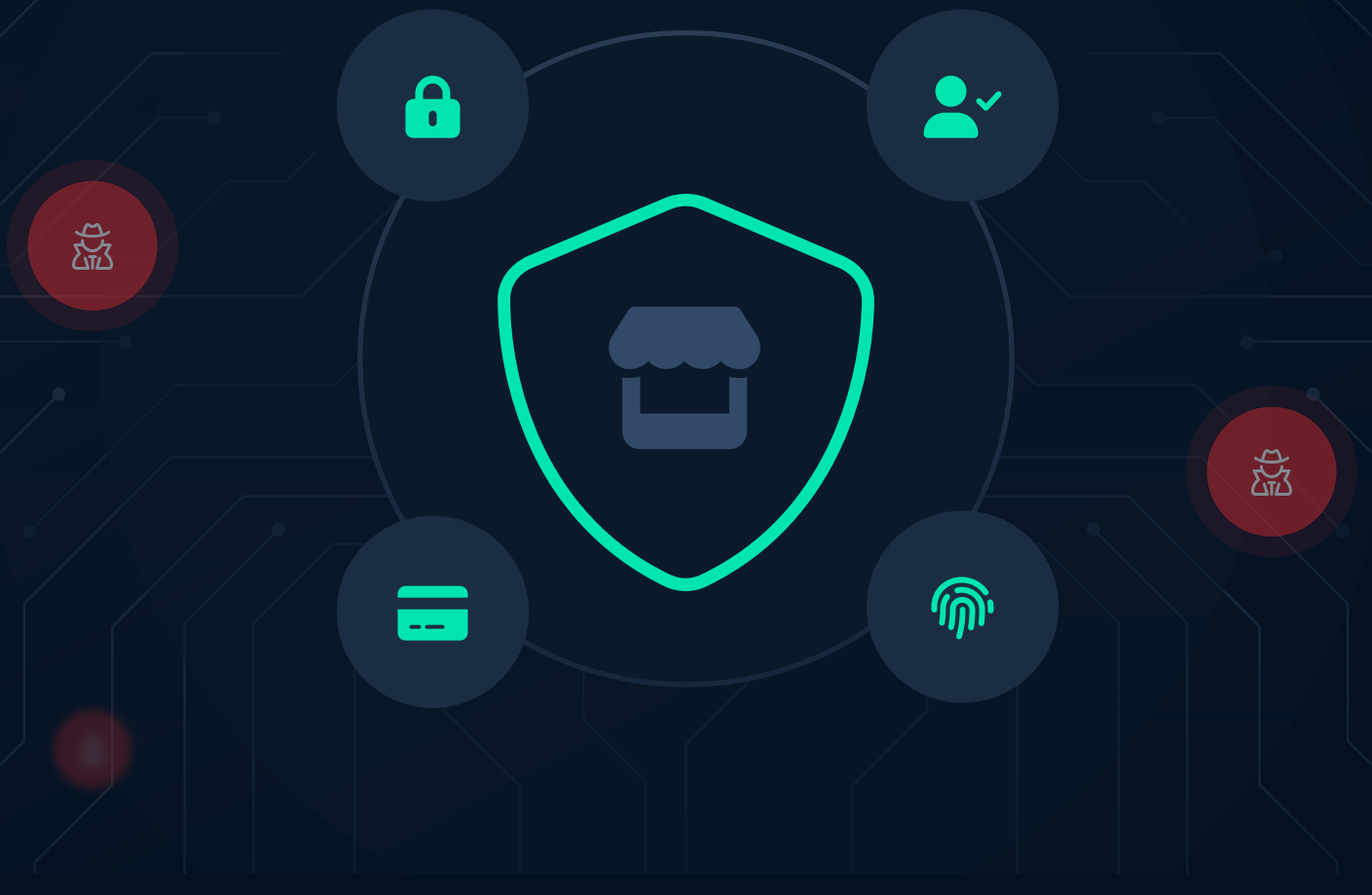
NOFRAUD

What Fraudsters Want: The Anti-Fraud Guide to Protecting eCommerce

Protect your eCommerce business from fraud losses.



Get in touch with a Fraud Expert. 888-773-3669 sales@nofraud.com nofraud.com

Contents

Chapter 1

Foreword — 3

Chapter 2

What Fraudsters Want — 4

1. System Gaps Between Subscription and Fraud Prevention Platforms — 4
2. High-Volume Products — 8
3. Access to Sensitive Information — 13
4. An Unsecure Payment Gateway — 21
5. Overburdened Staff — 27

Chapter 3

About NoFraud — 33

Foreword

> Fraudsters have been around since the beginning of time. But, as technology advances, more opportunities for fraud emerge, and schemes become increasingly sophisticated. According to the Federal Trade Commission, 2022 saw a **30% increase in consumer losses due to fraud compared to the previous year.**

Experts point to three primary motivations behind fraudulent activity: opportunity, rationalization, and pressure. The ever-growing eCommerce landscape has increased opportunities for fraudsters with more retailers moving their businesses online. Fraudsters love eCommerce fraud because it's so easy to scale their operations once they find a loophole that they can exploit over and over again.

Unfortunately, today's economic challenges are adding to financial pressures and fraudsters are finding it easier to rationalize their crimes. They may feel guilty stealing someone's identity, but will ultimately justify fraud thinking the cost mostly falls on a faceless company that can afford small losses.

Despite varying motivations and justifications, fraudster tactics are all the same. Fraudsters are looking for financial gain, so they target shops with vulnerabilities to exploit and products they can easily obtain and sell illegally. In this guide, we'll focus on the mindset of a fraudster — what signals your shop might send to make it a good target for fraud, the schemes fraudsters will put into play to attack, and what you need to do to protect your shop.

What Fraudsters Want

1 Fraudsters Want System Gaps Between Subscription and Fraud Prevention Platforms

The subscription boom has introduced new technologies designed to support the unique needs of selling subscription-based products on eCommerce platforms. With this, there has been a growing number of fraudsters exploiting loopholes, or vulnerabilities, in the integrations between subscription and eCommerce platforms.

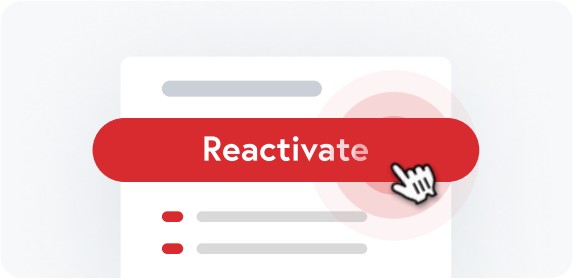
System gaps between subscription and fraud prevention platforms mean the right information isn't being passed to effectively detect and prevent fraudulent orders. A common issue with subscription integrations is that the tools might not pass along IP addresses. The IP address provides numerous fraud clues and, without it, it's hard to make accurate fraud decisions. An IP address tells us where an order was created, and fraud prevention software will look at the distance between the IP, billing and shipping addresses.

How do fraudsters target this vulnerability?

Scenario A:

Fraudsters use an IP proxy to hide their location.

When looking at an IP address, it's important to see whether or not there is an IP proxy. It doesn't always indicate fraud, but it can indicate the fraudster knows that fraud detection software is looking at IP addresses. If an IP is masked, merchants won't be able to determine from where the order originated and there's less visibility into the risk of the order.



Scenario B:

Fraudsters reactivate a canceled subscription.

Another vulnerability is when a subscription company allows for subscriptions to be reactivated. Fraudsters exploit this by reactivating a canceled subscription unbeknownst to the customer. Since many merchants don't have a fraud solution that screens recurring orders, the next order ends up getting shipped out, whether fraudulent or not.

What can you do to protect your shop?

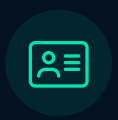
To mitigate the risks associated with system gaps between subscription and fraud prevention platforms, merchants should consider the following measures:

Seamless Integration:

Ensure that the subscription platform and fraud prevention system are properly integrated and communicate effectively. This allows for real-time data exchange, fraud alerts, and coordinated actions to prevent and detect fraudulent activities.

Robust Identity Verification:

Implement robust identity verification measures during the account creation process to ensure the legitimacy of shoppers. This includes multi-factor authentication, identity document validation, and data crossreferencing to detect and prevent identity theft.



Real-Time Monitoring:

Implement robust identity verification measures during the account creation process to ensure the legitimacy of shoppers. This includes multi-factor authentication, identity document validation, and data crossreferencing to detect and prevent identity theft.

Regular System Updates:

Keep both the subscription platform and fraud prevention system up to date with the latest security patches, software updates, and industry best practices. Regularly review and enhance fraud prevention measures to address emerging threats and vulnerabilities.

Collaboration and Intelligence Sharing:

Foster collaboration between the subscription platform and fraud prevention system providers to share threat intelligence, trends, and best practices. This helps in staying ahead of fraudsters and continuously improving fraud prevention strategies.

2 Fraudsters Want High-Volume Products

If you're selling products by subscription, chances are this attracts fraudsters. Highvolume products indicate high demand, which fraudsters see as an opportunity to easily sell the products themselves. The high demand also tips fraudsters off to the idea that their fraudulent orders may slip through the cracks and avoid detection by the shop.

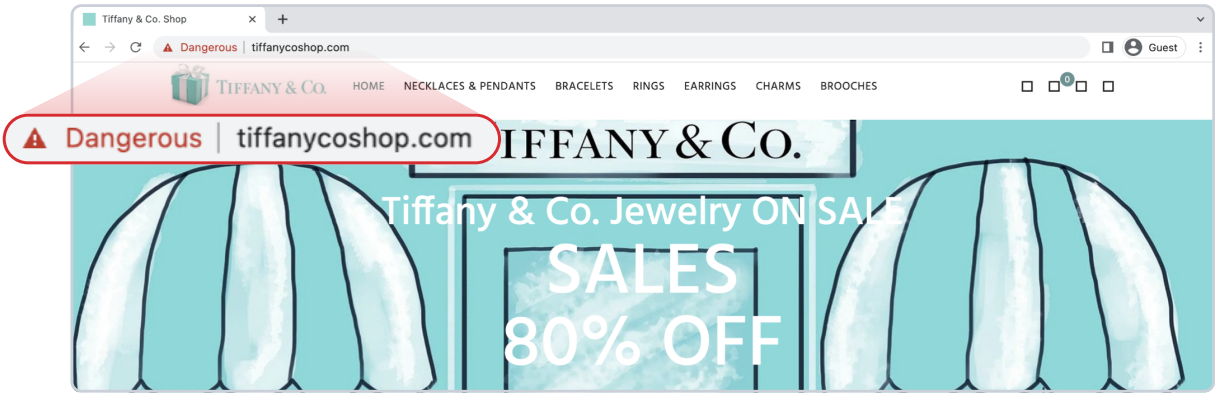
Fraudsters will steal images and descriptors of high-volume products and place them on their own fake online storefronts that are designed to mimic legitimate eCommerce shops. As many as 5,300 new malicious websites were launched per week, in the weeks leading up to the 2021 holiday season. Fraudsters are attracted to the easy turnaround of products and the lack of warehousing needed to run the scheme.

How do fraudsters target this vulnerability?

Scenario A:

A triangulation fraud scheme with a fake storefront.

Triangulation fraud involves three parties: the fraudster, the unsuspecting legitimate customer and the eCommerce store. Within the last year, NoFraud has seen a 70% increase in triangulation fraud. Fraudsters will target shops with high-volume products by creating a fake online storefront and listing the goods for sale at a 20-30% discount. They take advantage of the fact that the merchant has a popular product and customers will likely bargain hunt, which makes their fake storefront so appealing. When the fraudster receives an order through their fake shop, they will use a stolen card to make a purchase on the brand's website and input the shipping address of the fraudster's "customer."

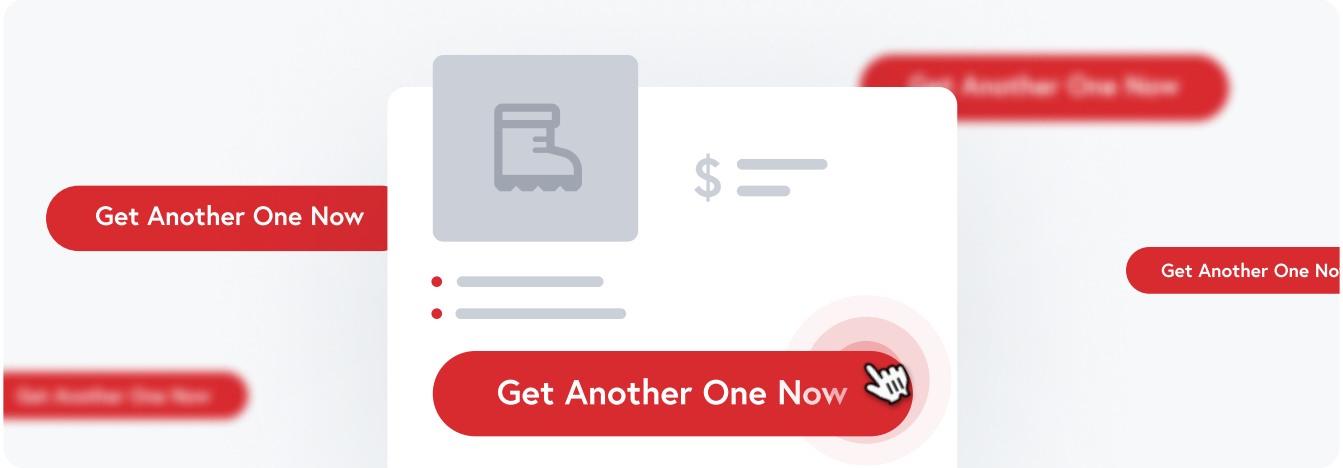


This fake online store leverages branding elements of the real Tiffany & Co. website. However, the URL is clearly fake and flagged as unsafe. The unusually steep discounts advertised are designed to lure shoppers in — another sign of a fraudulent site. Consumers who place orders on this site are handing over their personal details and payment information. When they find out they aren't receiving legitimate Tiffany jewelry (if they receive anything at all), they won't be happy and will have a negative experience with the brand.

Scenario B:

Fraudsters place multiple "get another one now" orders

Some subscription companies offer a "get another one now" button where customers can make another quick purchase if they run low on a subscribed product — before their next month's delivery. While an important and valid button to have for legitimate customers, fraudsters have realized that many companies don't have rebills screened. They'll put one order through and hit the "get another one now" button multiple times in a row.



What can you do to protect your shop?

To mitigate the risks associated with fraud targeting high-volume products, businesses can take the following precautions:

Vigilant Monitoring:

Regularly monitor online platforms, marketplaces, and social media channels for fraudulent listings or suspicious activities related to high-volume products. Promptly report any fraudulent activities to the appropriate authorities or platforms. If you're using a fraud prevention solution, it should be able to perform high-velocity checks and rebill reviews.

Brand Protection:

Brands should actively monitor their online presence, including monitoring for counterfeit products or unauthorized resellers. Implement brand protection strategies, such as trademark registration and enforcement, to mitigate the risks associated with brand reputation exploitation.

Secure Payment Processing:

Implement robust payment processing systems with fraud prevention measures, such as card verification, address verification, and transaction monitoring, to detect and prevent fraudulent transactions.

Strong Authentication:

Employ strong authentication mechanisms, such as two-factor authentication (2FA) or biometric authentication, to enhance security and reduce the risk of unauthorized access to customer accounts.

Customer Education:

Educate customers about common fraud schemes, such as counterfeit products, fake websites, and phishing attempts. Encourage them to purchase from trusted sources and verify the authenticity of the products and sellers.

3 Fraudsters Want Access to Sensitive Information

Fraudsters are focused on gaining access to sensitive information that they can abuse for their financial gain. This type of information can include PII, financial information, or login credentials. To do this, they look for entry points into the systems that hold this data and nearly 98% of the time it involves a social engineering scheme.

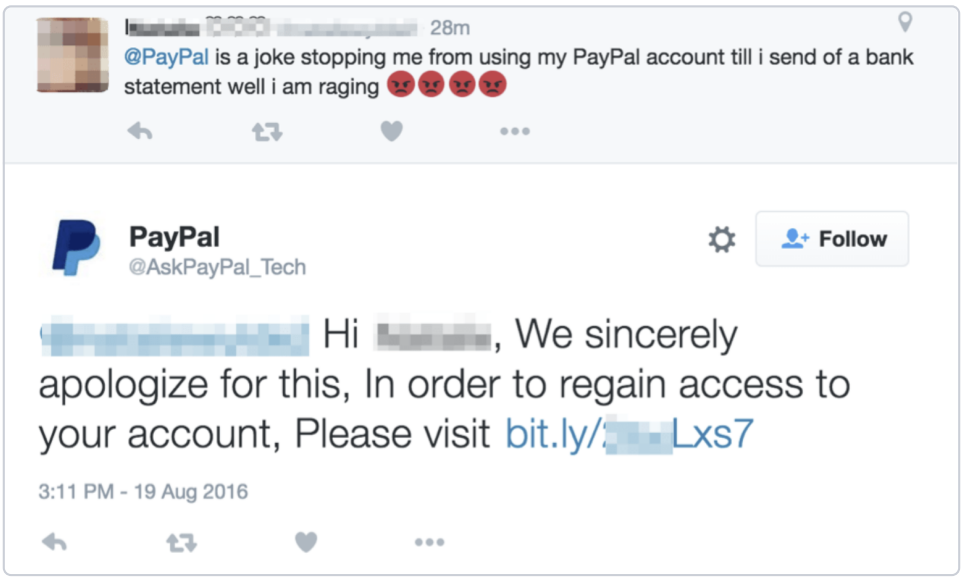
Social engineering is the manipulation of individuals to gain unauthorized access to information, systems, or physical spaces. It's a tactic often employed by malicious actors to exploit human vulnerabilities rather than technical vulnerabilities. The goal of social engineering is to deceive or trick individuals into divulging confidential information, granting access, or performing actions that benefit the attacker.

How do fraudsters target this vulnerability?

Scenario A:

Fraudsters impersonate brands on social media.

Angler phishing is a specific type of phishing attack that targets individuals through social media platforms. It involves the use of fraudulent social media profiles that often impersonate a company or a company's customer service team to deceive users and steal their personal information, login credentials, or financial details. The term "angler" refers to the way the attacker lures or "angles" the victim into falling for the scam.

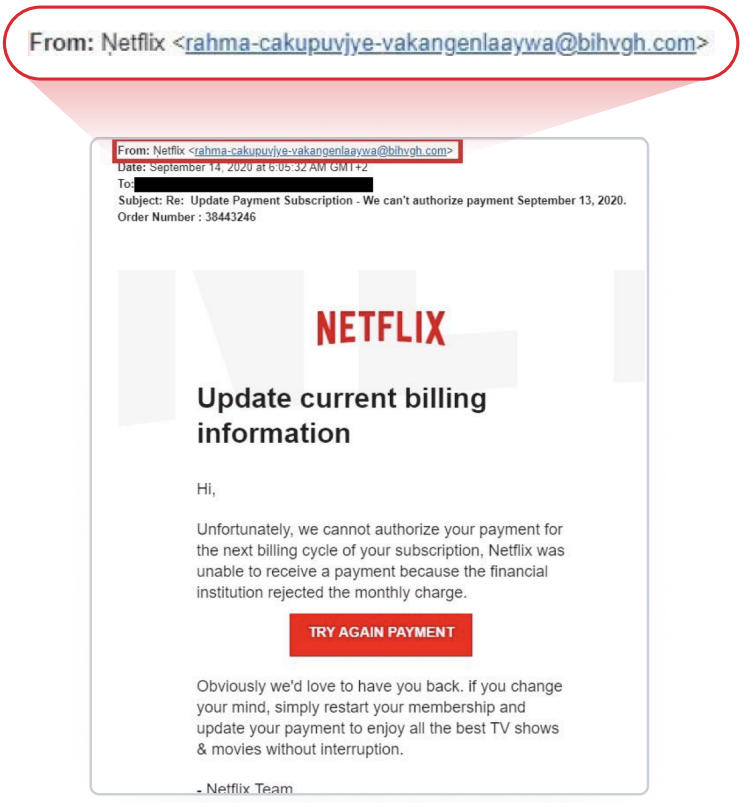


In this example, the user's handle @AskPayPal_Tech is a fraudulent Twitter handle posing as an extension of the PayPal customer service team. The fake account monitors Twitter for legitimate @PayPal customer complaints and jumps on replies in an effort to con dissatisfied customers into revealing private banking information.

Scenario B:

Fraudsters impersonate company employees or vendors via email.

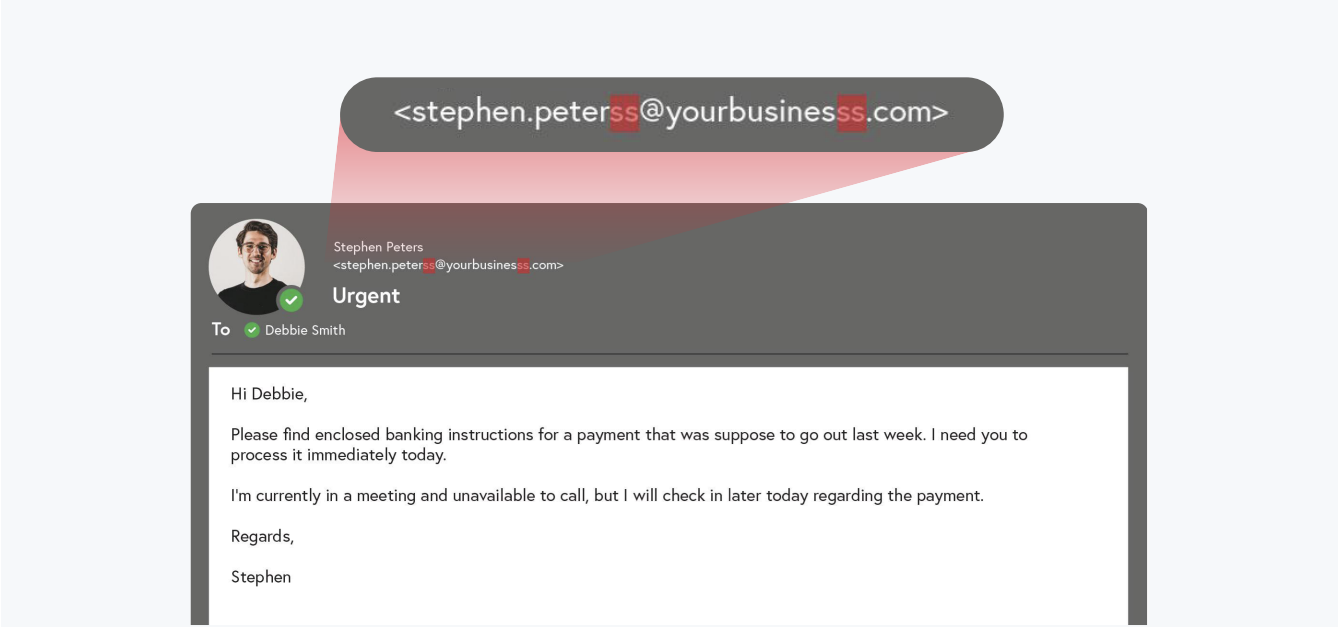
Angler phishing is a specific type of phishing attack that targets individuals through social media platforms. It involves the use of fraudulent social media profiles that often impersonate a company or a company's customer service team to deceive users and steal their personal information, login credentials, or financial details. The term "angler" refers to the way the attacker lures or "angles" the victim into falling for the scam.



An example of bulk phishing email

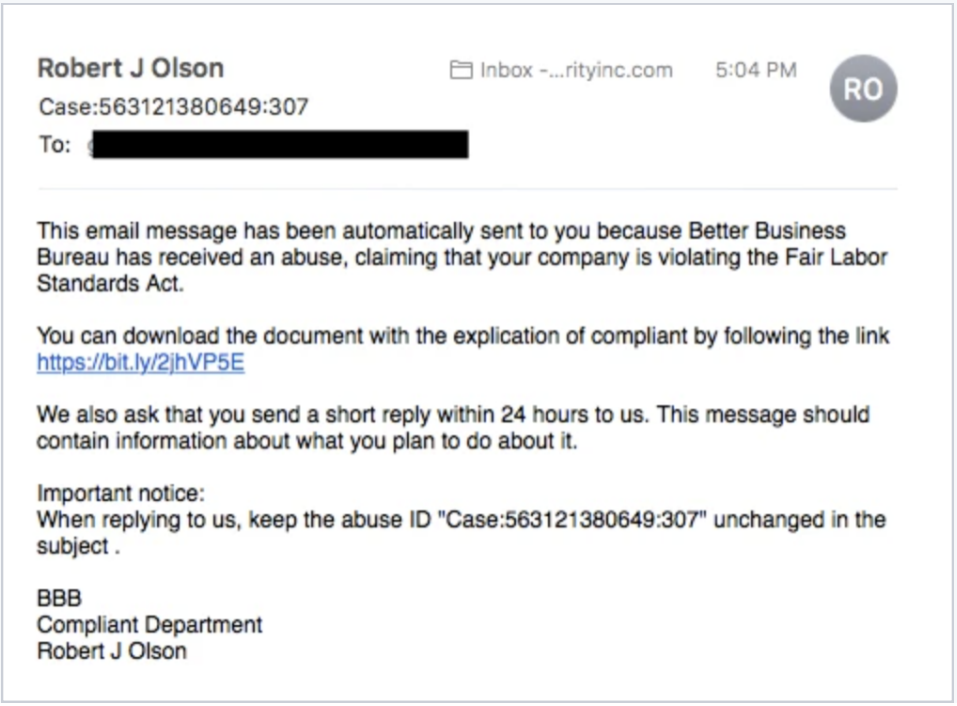
Whaling phishing, also known as whaling attacks or CEO fraud, is a highly targeted form of phishing attack that specifically targets senior executives or individuals in highranking positions within organizations. Attackers conduct thorough research on their targets, collecting information from public sources, social media platforms, and company websites.

By gathering personal information, phishers are able to tailor their attack and make it appear more credible, increasing the likelihood that the target will fall for it. This can lead to the victim sharing sensitive information, such as login credentials or financial details, or unwittingly authorizing fraudulent transactions.



An example of whaling phishing. Notice the errors in the sender's domain and deception tactic that plays on the employee's sense of urgency.

Spear phishing is a targeted attack that focuses on specific individuals, organizations, or groups of individuals. Attackers carefully select their targets based on various factors, such as their roles within an organization, their access to sensitive information, or their relationships with other individuals. The selection process often involves gathering intelligence through social engineering techniques, publicly available information, or data breaches. This research helps fraudsters tailor emails to appear as if they are coming from a trusted source or a known individual. Attackers may use the target's name, references to their job role, or specific details that are relevant to their work or personal life. This personalization increases the likelihood of the target falling for the scam.



Robert J Olson Inbox -...rityinc.com 5:04 PM RO

Case:563121380649:307

To: [redacted]

This email message has been automatically sent to you because Better Business Bureau has received an abuse, claiming that your company is violating the Fair Labor Standards Act.

You can download the document with the explication of compliant by following the link https://bit.ly/2jhVP5E

We also ask that you send a short reply within 24 hours to us. This message should contain information about what you plan to do about it.

Important notice:
When replying to us, keep the abuse ID "Case:563121380649:307" unchanged in the subject .

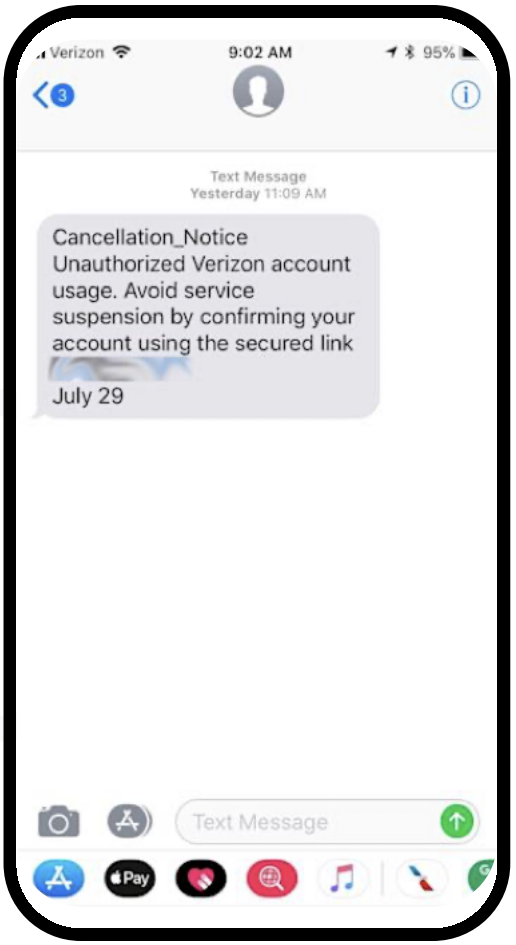
BBB
Compliant Department
Robert J Olson

An example of spear phishing.

Scenario C:

Fraudsters impersonate brands via text or phone.

Smishing and vishing are two types of social engineering attacks that exploit different communication channels: smishing targets SMS text messages, while vishing targets voice or phone calls. Much like the aforementioned phishing attempts, fraudsters employ similar tactics to deceive consumers and make them believe they are interacting with a trusted brand or organization.



An example of smishing

NOFRAUD

What can you do to protect your shop?

To protect sensitive information, eCommerce merchants can take the following preventive measures:

Secure Website Transactions:

Regularly monitor online platforms, marketplaces, and social media channels for fraudulent listings or suspicious activities related to high-volume products. Promptly report any fraudulent activities to the appropriate authorities or platforms. If you're using a fraud prevention solution, it should be able to perform high-velocity checks and rebill reviews.

Two-Factor Authentication (2FA):

Encourage customers to enable 2FA for their eCommerce accounts to add an extra layer of security and prevent unauthorized access even if login credentials are compromised.

Customer Education:

Educate customers about the risks of phishing, social engineering, and online scams. Promote awareness of safe online practices, such as being cautious of suspicious emails, avoiding clicking on unknown links, and verifying the legitimacy of websites before making purchases. Make it clear to customers what types of communication they can expect from your brand. If you send emails warning of account suspension, let them know which email address these communications will come from.

Fraud Detection Systems:

Implement robust fraud detection systems to analyze user behavior, transaction patterns, and risk indicators to identify and flag potentially fraudulent activities in real-time.

Data Protection:

Employ data protection practices, such as encryption, tokenization, and secure storage, to safeguard sensitive customer information from unauthorized access.

Regular Security Updates:

Keep eCommerce and fraud prevention platform software updated with the latest security patches and releases. Regularly test and audit the platform's security measures to identify and address potential vulnerabilities.

Fraud Monitoring:

Monitor transactions and user accounts for suspicious activities or signs of account compromise. Implement mechanisms to detect and respond promptly to potential fraud attempts.

4 Fraudsters Want an Unsecure Payment Gateway

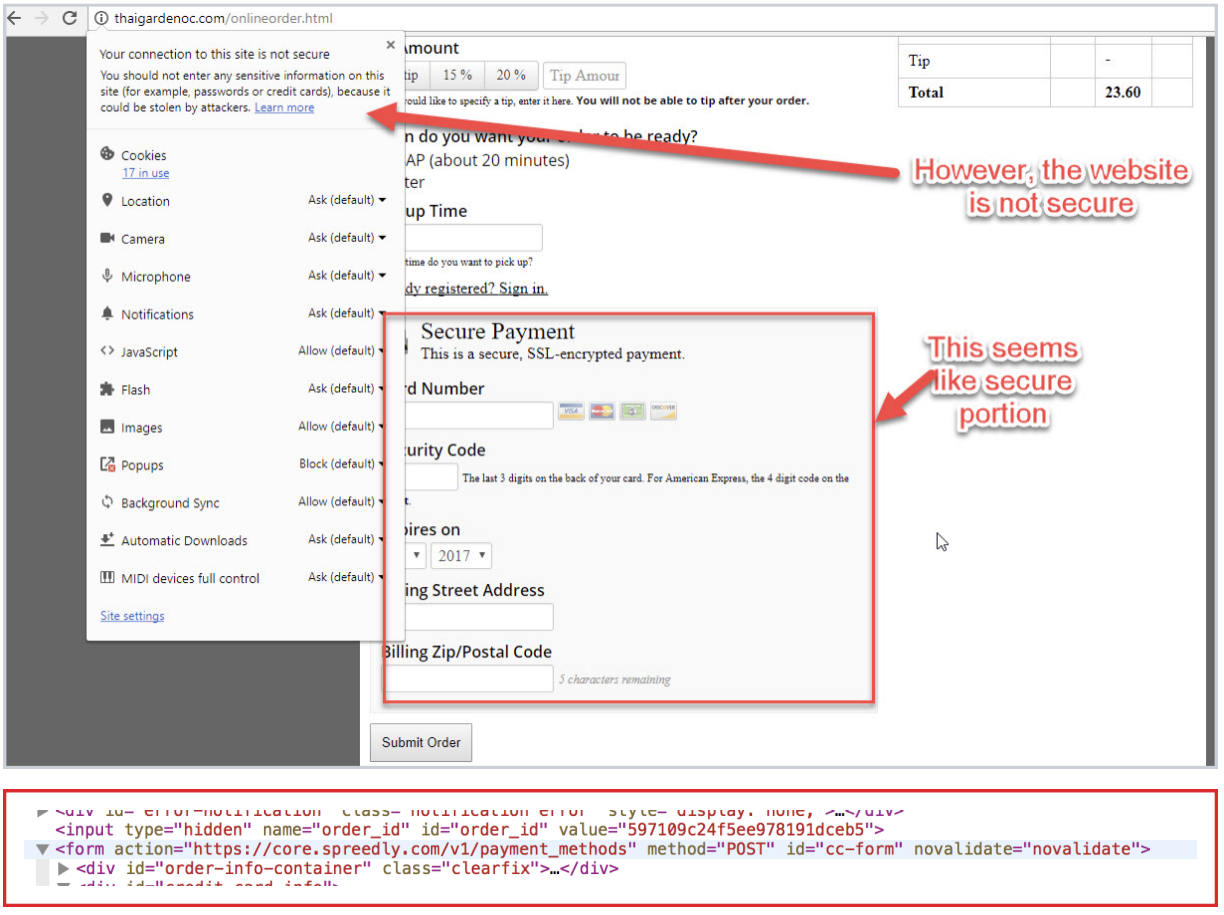
Payment gateways with proper security measures like encryption, secure socket layers (SSL), or multi-factor authentication are considered secure. These measures are put in place to protect consumers. Unsecured payment gateways do not have adequate security measures to protect sensitive payment information during transactions and leave consumers and businesses vulnerable to fraud.

Credit card fraud has been experienced by 65% of consumers at least once — a 7% increase from last year's reports. Without ways to authenticate and protect transactions over a payment gateway, fraudsters can easily use stolen payment information to make fraudulent purchases, unauthorized withdrawals, or fraudulent transfers of funds from the victim's account.

Scenario A:

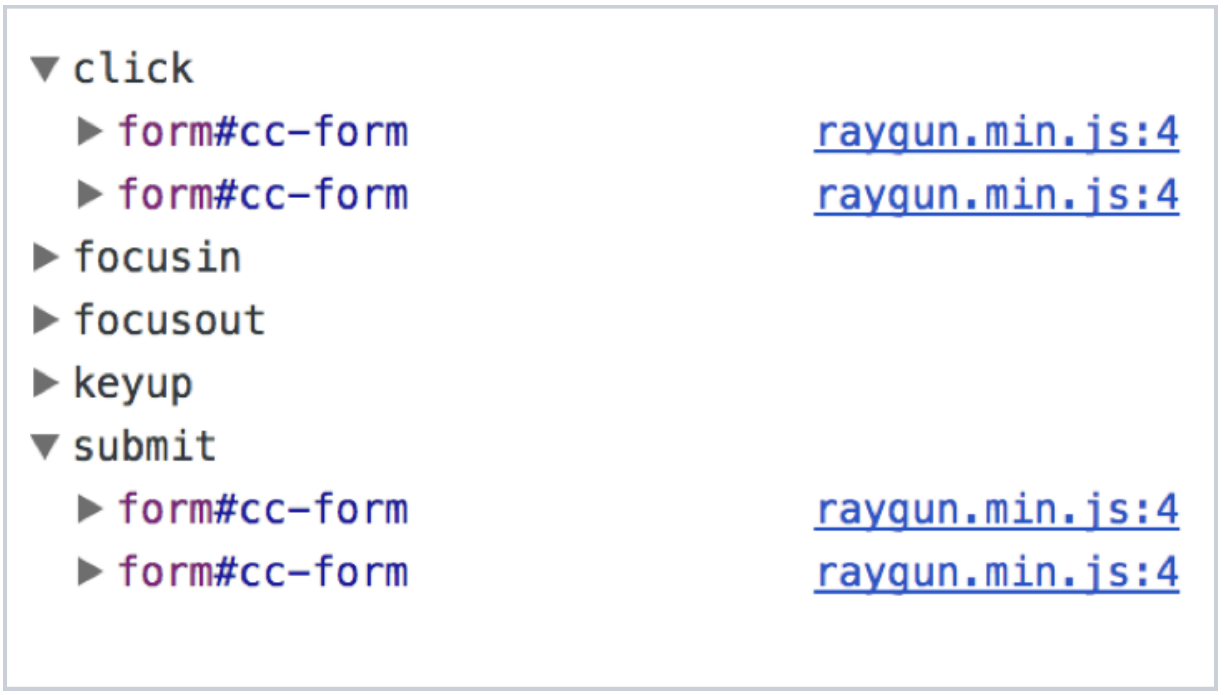
Fraudsters target non-secure websites.

Non-secure websites typically lack the necessary security measures, such as encryption and authentication protocols, to protect customers' sensitive information. Even with a secure payment gateway, a website that isn't secure leaves points of entry open for cyberattacks to hijack payment information before it posts to the merchant's site.



This website is loaded over HTTP, but the form itself posts to an HTTPS page.

However, the iframe that holds the form loads in HTTP, making it a non-secure transaction because the content of the iframe lacks integrity. This makes the page vulnerable to man-in-the-middle (MITM) attacks where fraudsters can reroute payments to another service.

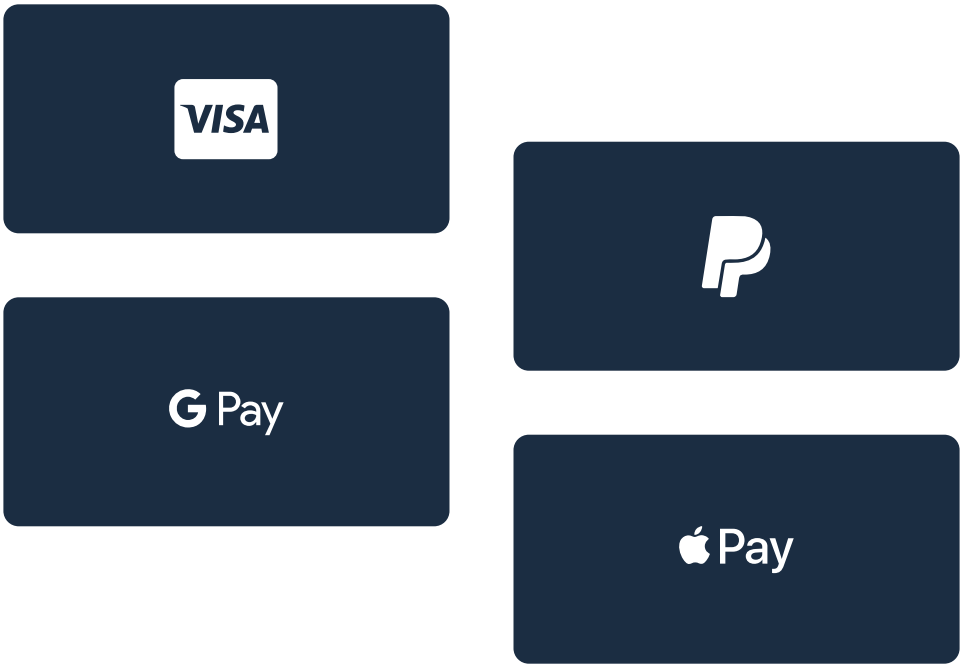


The form also has a click handler and submit handler, which leaves another avenue open for fraudsters to hijack the URL and change details before it posts. Cyberattackers will capitalize on this gap to steal your customers' credit card information.

Scenario B:

Fraudsters card test unsecure payment gateways.

Fraudsters use automated tools to systematically test large batches of usernames and passwords obtained from data breaches on unsecure payment gateways. The lack of security protocols and standard authentication allows fraudsters to gain unauthorized access to stolen accounts and conduct fraudulent transactions.



What can you do to protect your shop?

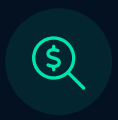
To protect against the fraudulent exploitation of unsecure payment gateways, merchants can take the following precautions:

Use Secure Payment Gateways:

Choose reputable and trusted payment gateways that employ robust security measures, such as end-to-end encryption, tokenization, and strong authentication mechanisms.

Regular Security Audits:

Conduct regular security audits of payment gateways to identify and address vulnerabilities promptly. Stay updated with the latest security patches and best practices recommended by the payment gateway provider.



Monitor Transactions:

Implement real-time monitoring systems to detect and flag suspicious transactions, such as unusual purchase patterns or high-risk transactions. This helps identify potential fraud attempts and take appropriate actions.

Payment Card Industry Data Security Standard (PCI DSS) Compliance:

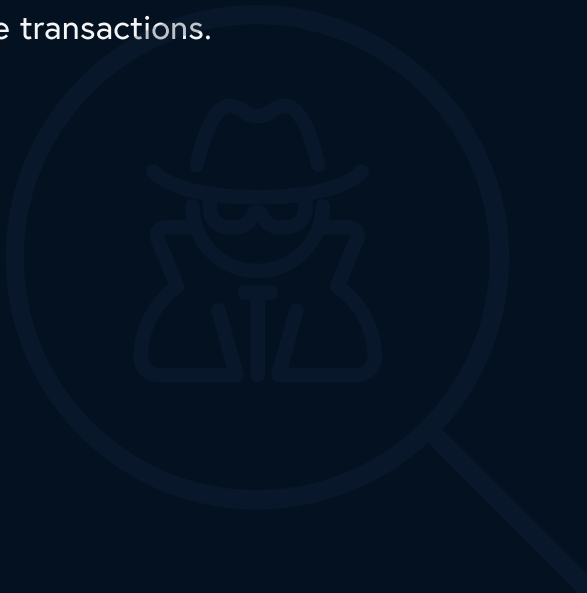
Ensure compliance with PCI DSS requirements, which outline security standards for handling payment card information. Adhering to these standards can help prevent fraud and protect sensitive payment data.

Educate Customers:

Educate customers about the importance of secure payment practices. Encourage them to look for secure indicators, such as padlock symbols or HTTPS in the website URL, before entering payment information.

Implement Strong Authentication:

Enable multi-factor authentication (MFA) or two-factor authentication (2FA) to add an extra layer of security to the payment process. This helps ensure that only authorized users can access and complete transactions.



5 Fraudsters Want Overburdened Staff

The holiday season provides fraudsters with unique opportunities to exploit the increased volume of online transactions, distracted customers, and overwhelmed businesses. According to Experian, one in four consumers have experienced fraud during the holidays — with 15% occurring on Cyber Monday.

When staff members are overworked, they become vulnerable to mistakes and may miss suspicious activities. As a result, they become easy targets for exploitation. Fraudsters realize that overburdened staff may not have sufficient time or resources to enforce and maintain strong security controls. Fraudsters take advantage of these weaknesses to bypass security measures, gain unauthorized access to systems or data, or exploit vulnerabilities.

Scenario A:

Fraudsters increase activities during the holiday season or during special promotions throughout the year.

Fraudsters target overburdened staff throughout the year. Aside from traditional holidays, any time your store runs a promotion, fraudsters see that as a signal that you're expecting a high volume of orders. They're thinking they can scale operations to take advantage of bigger opportunities, such as holidays or promo periods, and have a better chance of getting away with their criminal activities.

NOFRAUD

What can you do to protect your shop?

Is it the holiday season? Are you running a special promo? Fraudsters will come running. To reduce the risks of fraud during busy seasons, take the following precautions:

Increased Security Measures:

Enhance online transaction monitoring, identify red flags, and employ fraud detection systems to detect and prevent fraudulent activities promptly. Leverage a fraud prevention partner that provides a blended solution of platform capabilities and human expertise to approve more legitimate orders in real-time.

Timely Response and Incident Management:

Have a well-defined incident response plan in place to address any suspected fraud incidents promptly. This includes clear communication channels, escalation procedures, and cooperation with law enforcement if necessary.

Employee Training:

Educate employees about holiday-specific fraud risks, phishing attempts, and social engineering techniques. Provide guidelines on identifying and reporting suspicious activities.

Customer Education:

Raise awareness among customers about common holiday scams, safe online practices, and the importance of verifying the authenticity of websites and offers before making purchases.

Next Steps Checklist

Even as fraudsters implement the tools, technologies, and processes to scale operations and craft advanced schemes, the points of access can be controlled to mitigate any breaches. If you're wondering where to start, here's a step-by-step checklist to protect your shop.

1 Step 1: Secure Everything

- Check the integrations in your tech stack for system gaps.
- Implement encryption, firewalls, and other security protocols to safeguard sensitive information.
- Regularly update your systems to stay ahead of potential vulnerabilities and assure customers that their data is safe.

2 Step 2: Invest in Fraud Prevention

- Use a fraud prevention solution that plays well with your other technologies
- Partner with a trusted fraud monitoring service to help identify and respond to fraudulent activities in real-time.
- Regularly monitor and analyze transactions
- Respond quickly to security concerns and promptly report fraudulent incidents to the appropriate authorities.

3 Step 3: Make Fraud Education a Core Message

- Continuously educate customers on safety best practices that protect their accounts and data.
- Educate customers and employees about common warning signs of fraudulent activities, such as unsolicited requests for personal information, suspicious emails or phone calls, offers that sound too good to be true, and unusual account activities.

NOFRAUD

About NoFraud

Founded in 2014, NoFraud is an eCommerce checkout and fraud prevention pioneer, ensuring every eCommerce merchant has access to the services and protection they need to scale with confidence. The company provides online merchants with costeffective, easy-to-use solutions that remove friction and fraud from their eCommerce funnel to grow sales and improve the purchase experience for customers.

NoFraud provides the industry's most accurate eCommerce fraud protection solutions to increase merchants' conversion and approval rates while virtually eliminating fraud. Visit www.nofraud.com for more information.

Ready to learn more?

Set up a trial with a fraud analyst and see how NoFraud will benefit your business, by approving more orders, relieving your internal teams from manual review, and having a positive impact on your bottom line.

✓ Start a Free 2-week Trial Today

Get in touch with a Fraud Expert. 888-773-3669 sales@nofraud.com nofraud.com