Digitize + Thrive

PROTECT YOUR BUSINESS AGAINST FRAUD

How to stay ahead in the cybersecurity arms race

PayPal

WHAT IS THE FRAUD ECONOMY?

We used to think of online fraud as isolated incidents conducted by individual hackers and scammers. But in recent years, these types of cybercrime were increasingly conducted by coordinated and sophisticated networks of cybercriminals. Businesses must put in place protections which are just as sophisticated to protect themselves against fraud.

The pandemic changed the game in about every way possible, especially in eCommerce. The start of COVID-19 brought about a 60% surge in internet traffic, and as a result, spending by online shoppers nearly doubled[1]. Fast forward to 2021, fraud threats were worse than ever. eCommerce retailers were at risk of losing over $20 billion due to fraudulent online activities. This represented an 18% increase in fraudulent activities compared to the previous year[1]. Amid the stressful backdrop of the pandemic, fraudsters preyed on victims with charity scams, emails impersonating the World Health Organisation (WHO) or Center for Disease Control (CDC), and even robocalls pretending to be government organisations, distressed family members, or bank and credit card companies[2].

As the fraud economy continues to grow, so does the audacity of cybercriminals. They are getting smarter, more sophisticated and they now have greater access to the tools they need to exploit online businesses. They're just as, if not more knowledgeable about the mechanics of eCommerce as the businesses they target. This allows them to accurately identify security vulnerabilities and exploit them with the element of surprise[3].

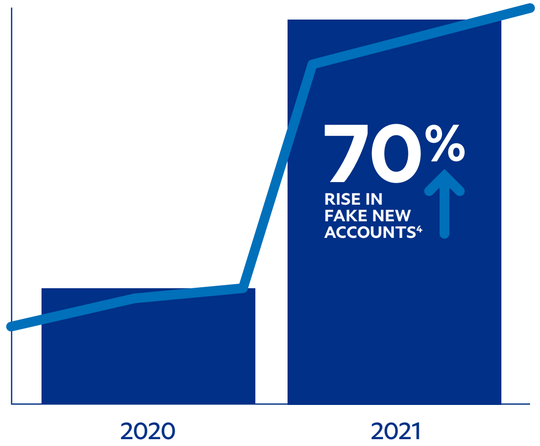
While fraud is running rampant, businesses are working harder than ever to keep up, but that doesn't mean customers' expectations have changed. Online shoppers still expect a fast and frictionless experience on top of air-tight security. If purchases take too long, require too much data, or are too complex, they abandon their carts and move on. These expectations make it challenging for retailers to meet their needs while also keeping their businesses safe against various cyberthreats.

1. Payments Dive, E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds, April 30, 2021. **2.** CyberCrime Support Network, COVID-19 Scam Alerts, April 12, 2021. **3.** Sift, Exposing the Multi-billion Dollar Fraud Economy, Q1 2021.

BUSINESSES ARE FACING NEW CHALLENGES WITH FRAUD WORLDWIDE

INCREASE IN NEW ACCOUNT FRAUD

In 2021, fake new account registration rose by over **70%**[4].



BOLD MOVES TOWARD BIGGER TARGETS

Each fraudulent purchase is on average **70%** higher in value than they were pre-pandemic[5].

THE RISE OF MOBILE ATTACKS

50% of all digital traffic was mobile and the mobile attack rate was **24%** in the first half of 2021[6].

4. Business Wire, 70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports, August 5, 2021. **5.** Retail Week, Every day is now Black Friday – and retailers need to prepare, November 4, 2021. **6.** Security Boulevard, Here's How to Fight Diverse Attacks Across Multiple Touchpoints, October 8, 2021.

STAY ONE STEP AHEAD OF CYBERCRIMINALS

With cyber threats more complex and prevalent than ever, businesses can no longer simply consider fraud as the cost of doing business. Last year, omnichannel retail saw a 50% YoY increase in fraud rates and a 9% YoY increase in fraudulent order volume[7]. Businesses should focus on having the right infrastructure in place to protect themselves against fraud.

5 Tips for Keeping Your Business Safe:

1. Monitor your site for suspicious activity
2. Stop cybercrime at checkout
3. Encrypt your data to keep payments safe
4. Update your software to level up your security
5. Know your blind spots to boost cyber strength

7. Sift, Exposing the Multi-billion Dollar Fraud Economy, 2021.

1 MONITOR YOUR SITE FOR SUSPICIOUS ACTIVITY

Suspicious activities can cost your business time and money but they aren't always easy to detect. It pays to be vigilant, so here are some ways to keep a watchful eye on your site.

Be wary of excessive chargebacks. Chargeback claims for unknown or forgotten purchases and a misunderstanding of return policies may be an indication of chargeback fraud (also known as friendly fraud or first-party fraud). 94% of businesses still see friendly fraud as an issue[8].

You can identify the tell-tale signs of unusual buyer activity by watching out for an address in an unfamiliar market and paying attention where billing and shipping addresses do not match. Also, be wary of suspicious email addresses, undeliverable emails, unusually large orders, or multiple credit cards used for one order.

Even as you pay more attention to your site activity, it never hurts to turn to the experts. If possible, outsourcing your chargeback management to a third-party specialist can take the burden of monitoring these patterns off you and your staff. There are also tools available that trace customers' IP addresses and alert you when they're from high-risk locations.

The PayPal Commerce Platform's fraud prevention and seller protection capabilities can help with this by implementing machine learning that adapts to your business to minimize chargebacks and covers you when certain fraud activities arise.

8. Business Wire, 8 Out of 10 Merchants Have Seen an Increase in Friendly Fraud, According to the 2021 Chargebacks911 Field Report, June 2, 2021.

2 STOP CYBERCRIME AT CHECKOUT

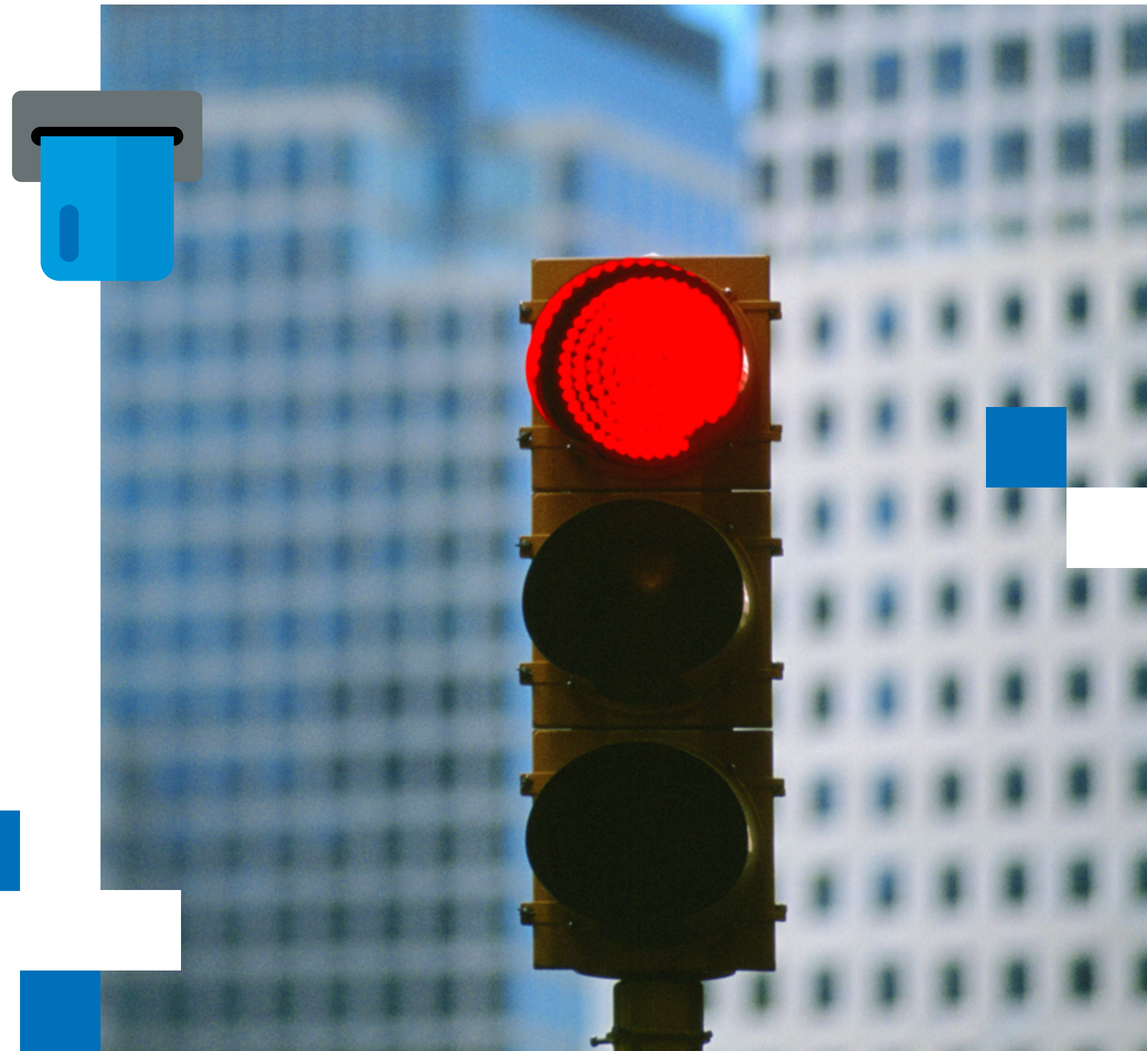
59% of businesses saw an increase in fraud due to card-not-present transactions, but fraud protection solutions at checkout can help you get ahead of these types of attacks[9].

1 in 4 merchants are struggling to implement payment security solutions, but taking these steps is essential as businesses test the waters of eCommerce[9].

Requiring Card Verification Value (CVV) numbers makes it virtually impossible for cybercriminals to commit card-not-present fraud since PCI rules prevent customers from storing their CVV with their credit card number. This ensures the customer has the physical card in their possession to make a purchase[10].

Address Verification System (AVS) helps you identify suspicious activities by comparing the numeric parts of the billing address associated with the credit card to the address on file with the credit card company. AVS is included in most payment processing systems as well, but it's still a good idea to check with your payment processor to make sure it's supported.

Lastly, velocity check is a fraud prevention mechanism that allows you to limit the amount of money or transactions coming from one customer per day. You can set any threshold that makes sense for your business and get notified when someone attempts to exceed it, or even have the transaction automatically cancelled. This is typically done to avoid fraudsters who are attempting to max out stolen credit cards.



9. Payments Dive, Merchants say they're losing revenue to online fraud, FIS report finds, July 12, 2021. **10.** Big Commerce, Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide.

3 ENCRYPT YOUR DATA TO KEEP PAYMENTS SAFE

Unencrypted data is a cybercriminal's best friend. It gives them easy access to credit card numbers, passwords, and more. Although there is a shift towards higher-value targets, many cybercriminals still prey on these easy opportunities.

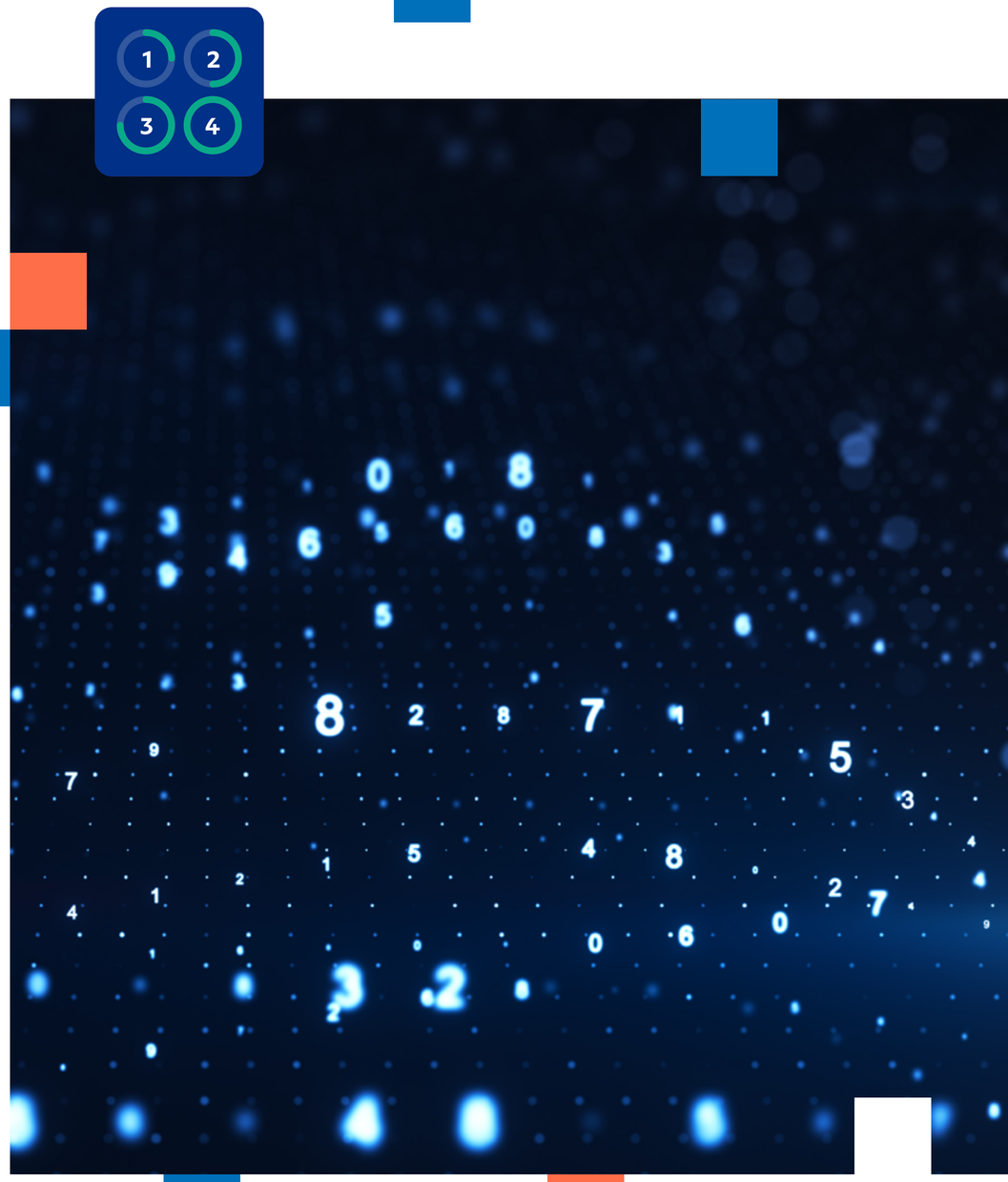
A massive amount of sensitive data is sent over the internet every day, so the possibility of it falling into the wrong hands is high, but there are steps you can take to make sure this won't harm your business or your customers.

End-to-end encryption technology prepares you for these situations by converting data into secret code before being sent over the internet. It's also a necessity for any business that stores or shares data due to both privacy and local data protection laws[11].

Take it a step further and ensure you have secure HTTPS connections using strong Transport Layer Security (TLS) configurations. TLS configurations are the current industry standard and let your information travel across the internet securely.

Make sure that your payment partner takes the security of your data as seriously as you do by complying with stringent data protection requirements.

PayPal's payments platform is backed by some of the best end-to-end encryption. From TLS and HTTPS connections to key pinning, these practices comply with stringent requirements that protect data in transit and at rest.



11. Insurance Business Magazine, Ten ways to protect your business from cyber attacks, March 20, 2021.

4 UPDATE YOUR SOFTWARE TO LEVEL UP YOUR SECURITY

Outdated software is one of the easiest ways for cybercriminals to crack into your systems[12]. Here are some measures you should take to close this open-door policy you didn't know you had with cybercrime.

Although keeping your operating system (OS) up to date is a simple and effective way to add a layer of protection to your business, 95% of websites still run on outdated software with known vulnerabilities[13]. OS providers are continually updating their systems with security patches to stay ahead of the newest threats, viruses, and malware. Even the smallest OS update can make a big impact on your business' security[12].

Business-grade anti-malware and anti-spyware software is another way to prevent attacks that target outdated software vulnerabilities—and you should keep these regularly updated too[14]. It's also worth noting that free, limited, and customer-strength software are insufficient because of their limited functions and coverage for business needs, possibly costing you more in the long run.

12. Business 2 Community, Top 5 Risks of Using Outdated Software in Your Company, June 14, 2021. **13.** Cybernews, 95% of websites run on outdated software with known vulnerabilities, March 18, 2021
14. Business 2 Community, 6 Ways to Keep Your Business Data Safe, October 26, 2021.

5 KNOW YOUR BLIND SPOTS TO BOOST CYBER STRENGTH

Cybercriminals are thieves of the future. They know how to leverage technology and innovation, but like an old-school pickpocket, they target a victim's blind spots. For example, when internet traffic swelled in the gaming and crypto space, cybercriminals knew that risk teams would be too overwhelmed by the traffic surge to catch them all[15].

Cybercriminals use sophisticated strategies to carry out wildly profitable attacks, so being informed and prepared is key. Know your vulnerabilities and most importantly, don't underestimate a cybercriminal.

One weak spot most businesses can relate to is high-traffic seasonal shopping events like Black Friday, Cyber Monday and Singles Day. Sales are soaring, but so are distractions and cybercriminals are aware that these distractions would be to their advantage.

At the other end of the spectrum, unusually low traffic can represent an opportunity for another blind spot. When the transportation sector experienced a significant dip in traffic due to COVID-19, cybercriminals went after dormant customer accounts for the rewards points and payment data[15].

Implementing the right protections during your busy season lets you enjoy your profits in peace—and keeping your guard up when business is slow takes opportunities away from fraudsters.

15. Sift, Exposing the Multi-billion Dollar Fraud Economy, 2021.

STRENGTHEN YOUR CYBERSECURITY WITH PAYPAL

The increase in eCommerce and cybercrime catapulted cybersecurity to the top of minds worldwide. As fraud continues to get more sophisticated and prevalent, a trusted payments partner is no longer just nice to have—it's essential. Partnering with PayPal gives you peace of mind with each transaction. Our powerful network securely processes more than 10 million payments a day and only gets smarter with each transaction. Get the tools you need to sell securely and confidently around the world.

Get Started →