E-Commerce Fraud is on the Rise.

Consumers and businesses alike need to be aware of the latest threats.

Since consumers first began purchasing items over the internet three decades ago, online retail shopping has become a vital sector of the global economy. Today more than 2.7 billion people - roughly a third of the world's population - routinely buy and sell things online. E-commerce sales accounted for more than 17 percent of overall retail sales worldwide in 2024 and are expected to make up more than a fifth of total global sales by 2029.

As e-commerce continues its upward trajectory, fraudulent activity associated with it is rising accordingly. Online scammers are constantly coming up with new ways to swindle individuals and businesses out of their money and merchandise, employing the most cutting-edge technologies available and sometimes even creating large, organized networks that mirror the corporate structures of the companies they're defrauding. This climate of anxiety can erode trust between online sellers and buyers, according to a 2024 Chubb report examining the trust dynamic between e-commerce companies and their customers.

In 2025, we can expect to see e-commerce scams evolve even further as cybercriminals take full advantage of developments in emerging technologies such as artificial intelligence (AI). Here's a look at where things stand right now - and where they may be headed.

Mapping the Current Risk Landscape

A 2024 Chubb report analyzing the impact of cyber scams on digital payments revealed two common tactics used by online scammers to defraud purchasers.

- In scams involving fake products or services, cybercriminals pose as real online merchants and vanish into thin air once payment has been made through a legitimate peer-to peer (P2P) payment app, leaving the customer without whatever product or service they've just paid for – but leaving the scammer with the victim's personal information, including their credit card or banking information.
- In formjacking scams, a criminal hacks into the website of a legitimate retailer using JavaScript code and redirects a customer to a fake payment form, where the hacker can then obtain the customer's personal and financial information.

Purchasers aren't the only victims of e-commerce scams; merchants are frequent targets as well. The commerce protection platform Signifyd notes that fraudulent orders placed to online merchants increased by 19 percent in the first half of 2024 compared to the previous year, while cases of attempted re-shipping fraud – in which criminals enlist the aid of accomplices (who may or may not be unwitting) to receive ill-gotten goods at their own address and then re-ship them, in new packaging, to a different address provided by the criminal – were up by 50 percent. The latter is seen as a sign that e-commerce crime rings may increasingly be relying on go-betweens to mask their role in online orders while moving stolen goods. Indeed, evidence suggests that scammers are growing more comfortable bringing outsiders into their criminal enterprises. Some professional fraud rings now even provide fraud as a service, orchestrating merchandise return-and-refund schemes on behalf of paying customers in exchange for a cut of the profits.

Increasing Sophistication and Game-Changing New Technology

Generative AI has the potential to dramatically simplify workloads by speeding up and streamlining processes. That holds true for cybercriminals, too. With the aid of this rapidly developing new technology, fraudsters engaging in fake products/services scams are getting better at mimicking the design and user-experience attributes of real online retailers, such that even consumers who are confident about their ability to detect a phony website can be fooled into believing they're dealing with an established, trustworthy brand. Many of the latest web design platforms use AI to create customized websites in a matter of seconds, and scammers are taking advantage. Unlike some of their pre-AI ancestors, these polished and highly sophisticated sites are much better at confounding people – and even at confounding other AIs that have been programmed to detect such fakery.

One form of e-commerce fraud that appears poised to grow in 2025 is synthetic identity fraud. In this type of scam, cybercriminals combine just enough real details about an actual person (such as their Social Security Number or home address) with completely fabricated ones to create a new online persona that can be highly difficult to detect as fraudulent. Using this synthetic identity, criminals are then able to establish fake credit records and successfully apply for merchant accounts, making purchase after purchase on credit lines – sometimes for months, or even years – before maxing out the credit lines and disappearing. Generative AI has sped up and simplified the process by which scammers create these identities by generating fake phone numbers, addresses and other personal details that can be used in their construction.

How Consumers and Businesses Can Protect Themselves

Consumers who want to keep one step ahead of today's cyber scammers can stay safer by taking the following precautions when shopping online:

- Check the URLs of trusted sites for tiny spelling deviations, a possible sign of typosquatting, whereby scammers create fake websites with URLs that look like the URLs of legitimate sites but are off by just one or two characters – and that rely for their efficacy on consumers not noticing.
- Check to make sure you haven't been redirected to an unsecured website at some point during your visit. (The URLs of secured websites will always begin with "https" – the "s" stands for "secured.")
- Plug the site into a reputable online site checker to verify its safety and legitimacy.
- Check to see if there are alternate ways of contacting the seller, such as a phone number or a physical address. If there aren't any, it could be a sign that something's not right.
- Look for any independent information you can find online that supports the seller's legitimacy (reviews, articles, etc.). Many scammers are highly adept at making realistic-looking websites, but don't take the extra time or trouble to create a larger universe of online information about their "company."

Meanwhile, online merchants can and should take precautions of their own:

- Implement zero-trust security architecture to minimize the risk of infiltration by cybercriminals or the introduction of malware into digital systems. Consider expanding zero-trust principles to interactions with customers, requiring them to use extra-strong passwords and/or multifactor authentication to access accounts.
- Carefully partner with only the most reliable, secure payment gateways that take extra steps (such as encryption or tokenization) to protect customer data.
- Monitor transaction activity constantly and closely for patterns suggesting the possibility of fraud: multiple orders from the same IP address, clusters of high-value orders, multiple failed login attempts or unusual chargeback volume.
- Use address verification service (AVS) and card verification value (CVV) checks to ensure that credit card numbers match credit card holder information.

Insurance As as Extra Layer of Protection

Insurance that can be obtained with the click of a button at the point of sale represents yet another way for customers and merchants to feel more secure when completing an online transaction. Because the option to purchase it is integrated seamlessly into the checkout process, embedded insurance doesn't require the customer to exit the platform in order to discover and research this protection: Buying tailored coverage to safeguard against specific risks – unreceived shipments or damaged merchandise, for example – simply becomes a natural, logical part of the purchasing journey.

Consumers seeking added peace of mind when making online purchases may feel safer conducting business with companies that provide this easy-to-use solution. For their part, merchants may find that providing it leads to several positive outcomes: improved customer satisfaction, enhanced brand reputation, simplified resolution of problems and disputes, and – with all these things – increased sales.

Looking Ahead

E-commerce scammers are getting smarter, employing ever more sophisticated methods for cheating people out of money and merchandise. But that doesn't mean that consumers and businesses can't avoid becoming victims of fraud.

By staying aware, adopting best practices and leveraging innovative insurance solutions, they can work together to outsmart today's – and tomorrow's – cybercriminals and protect themselves. To learn more about how Chubb can play a part in making online shopping more secure, visit pages detailing our digital products and other services that we provide for digital platforms.