
Mayo Studio via iStock

ECOMMERCE

The HEAT is on: cybercriminals hunt down web bargains

The rise of ecommerce in the pandemic has opened a lucrative avenue for cybercrime. Now businesses need to wise up to the latest methods of attack and strengthen their defences

David Stirling

Ecommerce came to the rescue of millions of us in the pandemic, be that new iPads to keep the kids busy or a hot tub for stressed adults. But the rush by firms to meet this wave of demand, whether they were a startup, an established ecommerce firm or a bricks and mortar store going online for the first time, left another group of people very happy as well: cybercriminals.

"Many businesses were forced to adopt new selling methods and ways of meeting customer expectations – on the fly," says Yoav Kutner, co-founder and chief executive of ecommerce platform Oro Inc. "At the same time, companies were focused on alleviating supply chain strains and cybersecurity fell a few rungs down the priority ladder. Hackers are now taking advantage because ecommerce sites are a treasure trove of personal data."

This includes online and email addresses when customers sign up to sites, as well as credit card details when they pay for their purchases.

Tom McVey, sales engineer at Menlo Security, says this data means ecommerce firms "have a target on their back". He also fears that many ignored basic security factors as they clamoured to drive sales. "The security maturity of a startup is not that high," he says.

Typical threats to ecommerce operations, he adds, include highly evasive adaptive threats (HEAT), which can bypass traditional security defences that include firewalls and secure web gateways. Menlo saw a 224% increase in HEAT attacks in the second half of 2021.

This can encompass smishing – which is essentially email-style phishing – but this time via text message. The principle is the same in that the hacker is trying to tempt a user to click on a link and unleash malware or ransomware onto a corporate or personal site. Traditional phishing remains a threat, with criminals taking advantage of vulnerabilities in new releases from Firefox or Chrome to launch browser attacks. Again, all you need to do is click on a link in an email for a browser to open and for a malware virus to be launched.

"We're also seeing double-dip ransomware," McVey adds. "Ransomware is where data on your system is encrypted by a criminal, and they refuse to unlock or decrypt it until a ransom is paid. But double-dipping is especially a problem for ecommerce firms because the hacker also steals their customer data, uploads it online outside the company's network and threatens to leak it. If that happened, your entire reputation would be ruined."

Jim Herbert is VP and GM for EMEA for global ecommerce platform BigCommerce. Other exotic sounding threats, he says, include SQL injections (where an ecommerce site insecurely stores data in a SQL database) and cross-site scripting (which involves inserting a piece of malicious code into a webpage). This exposes users to malware and phishing attempts. Another potential means of attack is e-skimming. This is when attackers steal credit card information and personal data by using phishing or XSS to access a site, then they capture a checkout payment in real time.

> **Companies were focused on alleviating supply chain strains and cybersecurity fell a few rungs down the priority ladder**

£56bn

Projected size of the ecommerce fraud detection and prevention market by 2025

GlobeNewswire, 2021

Cyber and online payment fraud is a further concern. According to Statista, global ecommerce losses in 2021 reached around $20bn (£16bn), an increase of more than 14% compared with 2020.

Abstract House sells original art and sustainable picture frames to customers via its website and was already established when the pandemic started. But it has seen the scale of threat, including fraud, increase over the past two years.

"We launched in 2017 and saw exponential growth in demand during the pandemic," says co-founder and CFO Summer Obaid. "People began to be comfortable about buying online, including art.

"That's been great for the business, but it has also brought interest from elsewhere. For years, we didn't see any fraudulent sales but now we're experiencing more such as people ordering several £500 gift cards. You may get one order like that but when it is multiple, we try to get more information."

The company, whose original paintings sell for up to £2,000, was aware that dealing with a huge amount of customer data made it vulnerable to attack. Its policy of proactively checking for anything concerning also applies to phishing emails, with employees encouraged not to click on external links and to delete them immediately. But it also has third-party help such as Shopify Plus, which uses machine learning algorithms to flag up orders that could be fraudulent. It also uses Google Business Suite to help protect against spam and secure private data in the cloud. In addition, data can only be seen by employees with privileged access.

McVey advocates web and email gateways to "keep the bad on the outside" and adopting the remote browser isolation model. This means that if an employee does click on a phishing link, there is no direct contact with a company's website and the malware won't run.

Herbert says firms should look at basic protections such as two-step authentication passwords, regularly upgrading software security updates, securing browser connections and ensuring that all connected devices are cyber secure with antivirus software and firewalls.

When it comes to payments, Obaid uses an SSL (secure socket layer) certificate on its website, meaning that all data is encrypted at checkout.

For McVey, it is the cloud – including cloud secure web gateways – which not only ecommerce but all businesses should be looking towards for better cybersecurity.

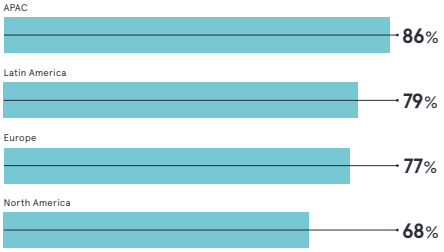
"It is rare for a company to store all its data at its premises nowadays," he says. "All of the documents, applications and emails which we now need to help more people work from home are on the cloud. But most company security strategies remain focused on the office and protecting that. There is a disconnect and little recognition that the world has changed. You can't have an office-based approach for a cloud-based world."

Another impact of hybrid working, McVey argues, and similar to the point Kutner made about the supply chain, is that a lot of IT spend has gone on making the transition as smooth as possible for employees. "Security has taken a bit of a back seat," he says.

Obaid says SMEs especially can't afford to let that happen. "It takes years for a company to build trust with a customer, but one negative experience can be a massive blow to your business. Cybersecurity is a real thing," she says.

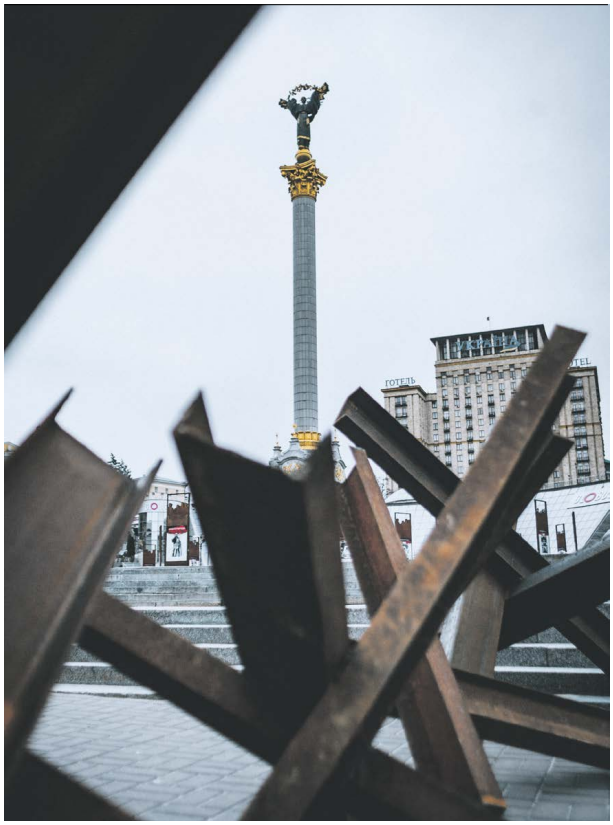
CYBER THREATS IN ECOMMERCE

Share of online merchants reporting increased fraud attempts due to the Covid pandemic worldwide in 2021, by region



Cybersource, 2021

Commercial feature



Shoring up cybersecurity amid a geopolitical crisis

The war in Ukraine has exposed the need for firms to have a robust cybersecurity strategy in place alongside a young talent pool

As the war in Ukraine continues to unfold, the world is becoming more geopolitically insecure. Global instability and uncertainty has heightened organisational risk for businesses.

One of the areas most impacted by this growing risk is cybersecurity. Cyberattacks have increased in severity and frequency as hackers have become more sophisticated in recent years, with such activity up 50% in 2021, according to technology security expert Check Point Research.

Ransomware is now one of the most common attack vectors. But a new breed of ransomware variant has surfaced that can't be stopped using traditional means and that's why it's imperative companies develop more robust cybersecurity strategies to prevent them.

Tackling global instability

"Organisations will need to review their security measures to defend against ransomware and other malware assaults," says Maurice Gibson, product manager, cybersecurity at global talent and reskill training provider mthree. "Executives have to be proactive and have a plan in place for what to do if their organisation is attacked. This will help them make decisions quickly and effectively without panicking and rushing during a crisis."

Global instability has created new employment challenges for firms. Among the biggest insider threats in the wake of the great resignation of 2021 are mid-career employees who quit, but still had access to valuable data and knowledge.

Added to that, the Covid-19 pandemic forced many organisations to move their workforce to remote work almost overnight. But because employees home networks often used devices outside of the company's monitoring and direct control, security can be more easily compromised. That has meant businesses have had to ensure workers' home networks are protected as part of their overall cybersecurity plan and protocols.

As many firms have been forced to change suppliers in different regions because of increasing geopolitical difficulties or disruptions, they have also had to do their due diligence and make sure any third-party providers they work with have cybersecurity practices that comply with their own.

"With geopolitical shifts in power, organisations are having to find new suppliers to guarantee their production domains can be maintained while reducing expenditures," says Gibson. "Organisations are engaging third parties who may or may not have gone through the same level of due diligence and are attempting to untangle connections with a third-party vendor in a less desirable geography."

Plugging the skills gap

A deeper issue is trying to find and retain employees with the right skills and tools for the job. And because technology is constantly evolving, so new talent is always needed, as well as continually updating the existing workforce's skillsets.

But as the relentless war for talent continues, current employees are being stretched to the limit, being required to do more and carrying out multiple jobs to cover the work that needs to be done if someone can't be recruited for those roles. This is evidenced by the fact that there are almost 465,000 unfilled cyber jobs in the US alone, according to US government-sponsored data. This can often result in burnout and workers leaving because they're fed up or can't take the pressure, workload or longer hours.

> **Rather than relying on certain locations to fill openings, junior talent can be found wherever the business is or where it wants to expand**

Despite the obvious problems this presents, it also provides employers with the perfect opportunity to turn it into a positive. By considering a wider range of candidate, in terms of age, gender, ethnicity and background, they can finally address this long-standing issue.

"This opens possibilities for employers to look outside of their usual recruiting pools when hiring technology professionals. Employers may benefit from sourcing various talents from different communities, which can lead to creativity and a better work environment."

Junior talent can also play a key role in helping meet employers needs amid disruption. "Junior talent may lead to more adaptability in organisations," says Gibson. "Rather than relying on certain locations to fill openings, junior talent can be found wherever the business is or where it wants to expand."

465,000

the number of unfilled cyber jobs in the US alone

Cyberseek and US Commerce Department, 2022

He adds: "Junior talent enables an organisation to develop its personnel from the bottom up, providing them the chance to apply their skills toward the company's benefit. Many companies are paying a premium for skilled employees in an expensive labour market. Junior talent allows firms to spend less up front and reinvest funds into training and upskilling opportunities that help reinforce talent retention."

Strategic risk management

In response to the war in Ukraine, as with any other international crisis, in addition to having a solid cybersecurity strategy in place, firms also need to test their business continuity and recovery plans to ensure they work and are up to date. They also need to find in-country talent or suppliers that will help them isolate themselves from the conflict's impact.

Linking all this together, organisations need to have established and effective lines of communication with suppliers, industry peers, governments and employees. They also need to look at the bigger picture in terms of the long-term impact on business and how they can mitigate that risk.

Moving forward, the need for better cybersecurity has never been greater. As a result, companies must re-evaluate their broader risk and business continuity strategies, ensuring they continue to comply with the latest set of data privacy and security regulations, as well as assessing current and emerging geopolitical risks, and how they will tackle them.