WHY ARE RETAIL BUSINESSES TARGETED BY CYBER CRIMINALS?

CYBERCRIME INDUSTRY SNAPSHOT

Retail

CYBER READY

mailguard

Cybercriminals exploit trusted brand names in the retail sector to send malicious emails

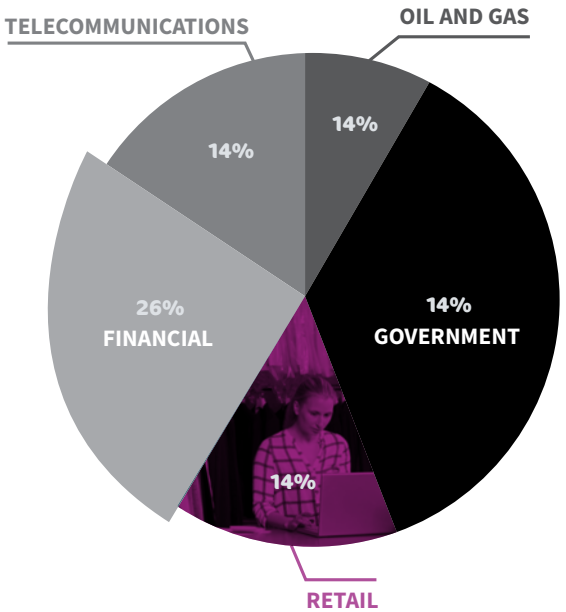
Amazon, eBay, and other eCommerce behemoths are rapidly outpacing traditional department stores in terms of growth and market capital. Customers freely volunteer their credit card and personally identifiable information (PII) online including date-of-birth, physical, postal and email addresses—all highly coveted information on the dark web.

Global and national retailers are household names and trusted brands. This makes it easy for cybercriminals to get click-throughs on email phishing campaigns and text messages by 'brandjacking' (brand hijacking) big retailers. The likelihood of email targets having a previous transaction or relationship with big brands is high. Receiving email notifications and text message updates from brands have become the accepted norm.

Internet of Things (IoT) in retail (including point-of-sale software, in-store cameras, smart shelves, inventory tracking, contactless payment leveraging Radio-frequency identification (RFID) and employee smart devices) are all potential exploits. Unsecure RFID, Bluetooth, public Wi-Fi and other wireless connections make retailers particularly vulnerable. A domain name provider cyberattack exploited unprotected IoT devices, causing massive outages to eCommerce customers Etsy, Shopify and PayPal in 2016.

SECTORS TARGETED BY INDUSTRY

Attacks on retailers account for 14% of all cyberattacks



Source: Control Risks' Cyber Threat Intelligence Report

HIGH PROFILE CYBERATTACKS IN THE RETAIL SECTOR

Total cost of Target's data breach in 2013

Data from **110 million customers** and **40 million credit card numbers** were stolen due to a spear phishing email. The breach went undetected for two weeks resulting in settlement claims totalling USD$18.5 million.

Phishing email enticed victims to complete a survey

Global cybercriminals are attuned to local markets and have no qualms about exploiting opportunities, coinciding this scam with Amazon's launch in the Australian market.

Technology in the retail sector is vulnerable to hacking

Point of Sale (POS) systems are particularly vulnerable due to varying standards in technology. POS data breaches increased from 22% to 31% in 2016. Ransomware is software that maliciously encrypts data and networks, enforcing victims to pay a ransom to the criminals behind the attack to regain access to their data and technology. Given the myriad of devices and other endpoints used in retail, ransomware poses a significant threat to merchants.

In 2017 a lakeside Alpine hotel in Austria was hit by a ransomware attack. Demanding a payment of two Bitcoins, cybercriminals warned the cost would double if the hotel did not comply with their demands by the end of the day.

The ransomware impact on the hotel was immediate, paralysing their reservation system and locking guests out of hotel rooms. Panicking, the owner caved in and paid the ransom in order to restore his business operations.

Although compliance with the Payment Card Industry Data Security Standard (PCI DSS) is improving among the sector, almost half (44.6%) of retailers and hospitality organisations are non-compliant—highlighting a huge vulnerability for the sector in protecting cardholders' data. The cybercrime cost to the retail sector is more than just financial. The cost to brand reputation and customer trust is immeasurable.

The cybersecurity landscape for the retail sector

Two in five global retailers were victims of a data breach in 2017 and a third of retailers were impacted more than once

Cybersecurity issues for the retail sector is heightened with the General Data Protection Regulation (GDPR). From May 2018 the GDPR enforced all businesses in the European Union (EU) to comply with new regulations to protect, strengthen and unify data protection for all individuals within the EU. Retailers need to act now and implement more robust data security solutions—including encryption, email and web filtering, data tokenisation, secure storage and authentication protocols—to protect the privacy of their customer base.

MailGuard reporting on recent phishing scams

As larger retailers, and, by association, delivery services and payment platforms, have significant customer databases, they are often victims of brand impersonation in criminal intent email campaigns. MailGuard regularly detects and blocks, phishing emails purporting to be from eCommerce giants Apple and eBay, as well as Australia Post and PayPal. MailGuard sees a seasonal spike in Australia Post branded email scams during Christmas, commensurate with online shopping volumes.

The emails are socially engineered to generate high click-throughs—with urgent or high interest calls-to-action such as a package delivery notification and changes in their account status. Even though recipients may not have recently transacted with the company, both brand awareness / affinity and curiosity, impel people to click.

Retail testimonials

CARPET STYLE CARPET COURT FLOORING CENTRE

"We were very impressed with our decision to implement MailGuard as our virus and spam filter. Our mail server load reduced significantly [and] we can now utilise our internet quota for more meaningful business purposes. We always received quick and prompt responses from [their support] team. Furthermore, we benefit from the comprehensive reporting which is always executed in a format that is easy to read and understand. The MailGuard experience has been well worth it."

—IT Manager, Carpet Court

Bakers Delight We're for real.

"We've noticed an incredible amount [of malicious email] has been stopped and that has certainly been well received by our user population.
From an IT point of view, we think it's great because it's less garbage in our server logs and less traffic we have to receive."

—Information Services Manager, Bakers Delight

GET CYBERREADY WITH MAILGUARD

We identify and stop fast-breaking attacks in real-time, 2-48 hours ahead of the market
Contact your IT service provider now for an obligation-free, 14-day trial

PHONE 1300 30 44 30
EMAIL expert@mailguard.com.au
WEB mailguard.com.au

CYBER READY

mailguard