WHY ARE FINANCIAL SERVICES A LUCRATIVE TARGET FOR ONLINE CRIMINALS?

CYBERCRIME INDUSTRY SNAPSHOT

Financial services

CYBER READY

mailguard

Financial services firms are a magnet for data theft and online fraud

The vast amounts of sensitive data and its proximity to money banks hold, and their heavy reliance on enterprise legacy systems, make them an obvious target for cybercriminals.

Put simply, it's where the money is. Add to the equation the data-rich nature of Financial Services Institutions (FSIs) who house highly-sensitive customer data and their bank account details—which can be hacked virtually from anywhere in the world, at any moment.

Whether it's a Direct Denial of Service (DDoS) designed to shut down a website by overwhelming it with traffic, a ransomware attack demanding money for access to hijacked systems, or a spear-phishing email scam orchestrated to make an unwitting million-dollar transfer to cybercriminals, security measures within FSIs are being tested thousands of times daily.

Cybercriminals and fraudsters will continuously attempt to disrupt operations, destroy critical infrastructure and gain unauthorised access to FSI funds.

Some high profile attacks

latest Equifax breach victim tally

stolen data included names plus social security, driver's license, and credit card numbers

drained from bank accounts

in a few hours during an infamous attack known as the Bangladesh Bank heist

thieves stole $US14 billion

from 14,000 Japanese convenience store ATMs in 2016

attacked online banking systems

worldwide in 2015 using sophisticated social engineering techniques

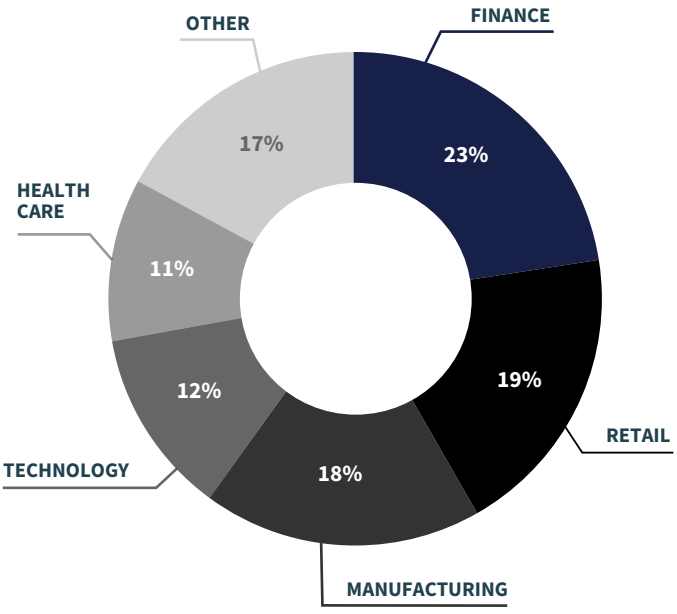
The cybersecurity landscape for the financial services sector

According to an IBM X-Force Threat Intelligence Index Report the industry was attacked more than any other sector in 2016 with a 29% rise in incidents—cyber events that actually or could potentially compromise the integrity of a system's data or operations. FSIs insiders are to blame for 58% of attacks against financial services clients. Of those insiders, only 5% of incidents were premeditated and malicious—the other 95% of were unintentional. Deloitte agrees: financial services tops its list of 26 industries that cybercriminals attack most frequently.

Banking and financial services ranks narrowly behind the energy sector as the most common target for DDoS activity, and the second-highest number of system compromises, according to the Australian Cyber Security Centre.

Fraud, including cyber-enabled fraud, is by far the highest reported threat to Australia's securities and derivatives sector representing 51% of the suspicious matter reports received by the government.

Typically, those incidences involved sending fraudulent instructions to a financial institution via a hacked email account, or the hacking of a customer account to conduct unauthorised trades, according to the Australian Transaction Reports and Analysis Centre (AUSTRAC).



Sectors targeted (% total attacks)

CYBERCRIME
MOST TARGETED SECTORS

Source: The Cybersecurity Place, 2016

stolen from a Bitcoin exchange

in 2017, totalling $US5 million and spreading the burden of the loss to their customers

swindled from user accounts

via the Hong Kong Bitcoin platform Bitfinex in 2016

MailGuard reporting on recent phishing scams

Due to the massive customer bases and brand equity of financial institutions, online scammers typically impersonate brands such as global or regional banks (ANZ, Commonwealth Bank of Australia, Barclays Bank, St George) and accounting software companies (Xero, MYOB).

Fraudulent email posing as financial services providers are highly effective because of the sensitivity and perceived urgency of banking, account and other financial matters. Examples of email scams are invoices and purchase orders, account notifications and overdue payment / debt collection notices.

Often, the intention of the malicious link or executable payload is credential scraping. On the dark web, the value of full credit card details is around USD24, and for online payment services logins up to USD200 per record, so a successful phishing campaign can be a boon for cybercriminals.

Business email compromise (or CEO fraud) is a rising threat, surging 130% and siphoning $22.1m in fraudulent transactions in 2017. These highly targeted, socially engineered scams typically target the CFO or other authorised finance manager within an organisation.

Financial services testimonial

FINDEX

"MailGuard has provided us with seamless protection and peace of mind since 2005 across our network of 80 offices and 2,000 employees in defence against spam, phishing and most recently, the new variants of malware such as CryptoLocker."

—Technology Services Group Manager, Findex

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