

Why Are Cyber Criminals Targeting the HOSPITALITY SECTOR?

Cybercriminals target restaurants because of the valuable data available

Just last year fast-food chain Wendy's disclosed it was a victim of a point-of-sale system attack that installed malware on PoS computers affecting **300 FRANCHISE RESTAURANTS.**



Statistics show the risks and potential impact are massive:

\$75,000:

Average cost to a restaurant for a data breach



50%

Percentage of restaurants who will go out of business within one year of a breach



1 in 8:

Number of restaurants that will suffer a breach event within the next two years



Thousands of W2s stolen from restaurant chain in email scam

Scotty's Brewhouse are working to inform **0000'S** of employees across the company about an email data breach, leaking employees' **W-2 FORMS** to an unknown suspect.



CEO FRAUD: THE NEW **\$2 BILLION**



Restaurants are frequently victim to CEO fraud emails

Statistics show that the spear phishing scam known as "CEO Fraud" has already racked up more than \$2 billion in losses and victimized **12,000 INDIVIDUALS**

globally. Losses have averaged a median of \$120,000 with the highest loss reported to be \$90 million.



What to look out for :

The greeting is different to the usual.



The tone is abnormal. It's an unusual out of character request.



There's an inconsistency in the typical chain of command



6 Essentials for Restaurant Network Protection from Hackers

To remain competitive, restaurants must ensure card processing, Wi-Fi access, loyalty programs and mobile payments are secure. Proven network security that defends against costly cyber attacks is crucial.



Encrypt your data.



Secure your hardware.



Lock your network – including Wi-Fi



Install anti-malware, anti-spam and anti-virus protection.



Keep your software up to date



Educate your employees.



Hire security.



Insecure Wi-Fi

Customers today are driven to locations that offer the best overall experience, not just the best food or service. Insecure Wi-Fi used by guests or employees, can allow unauthorized access to internal networks by Cyber criminals.

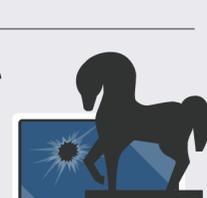


Kaspersky reported in November that over a quarter of public Wi-Fi hotspots, from around the world, were unsecure and posed an enormous threat to any user's data. 25% of the networks used no encryption, whatsoever.

KASPERSKY LAB

10 of the busiest malls in the USA had five or more risky Wi-Fi networks

Kaspersky reported in November 2016 that more than a quarter of public Wi-Fi hotspots, from around the world, were unsecure and posed an enormous threat to any user's data.



Open unfiltered Wi-Fi is an invitation to attack

An open unfiltered Wi-Fi network is an invitation to attack your users, data, privacy and data integrity.



A successful attack could result in:

Total loss of customer data privacy



Total loss of customer data integrity



Total loss of data customer confidentiality



In some parts of the world, it's illegal to not protect your customers' data



The company networks can be attacked by anyone using that network



Serious brand reputation and resulting costs and implications



Potential litigation



McDonalds and Starbucks have now introduced Wi-Fi filtering across their stores to **Block Porn and dangerous websites on their WiFi Networks.**



WebTitan can make your WiFi network safe by protecting your guests and employees from fraudulent 'phishing' Websites – sites that are made to look legitimate but are designed to trick people into entering personal or financial information.

Talk to a security specialist

email us at info@titanhq.com

with any questions.