CEO Fraud
What Every Executive Needs To Know

EMAIL SECURITY WHITEPAPER

What is CEO Fraud?

CEO Fraud, also known as Whaling or Business Email Compromise (BEC), is sophisticated email fraud designed to manipulate and extract payments from unsuspecting targets.

CEO Fraud attacks are sent as simple, well-crafted emails to specific people with authority to transfer company funds. The emails impersonate people of influence within an organisation, typically a CEO, CFO, MD or similar C-level executive.

This methodology makes it faster and easier to influence and trick individuals, enabling criminals to strike while reducing the likelihood of prosecution for their crimes.

To ensure emails appear authentic, criminals engage in 'social engineering'—researching and learning as much as they can about their target, the organisation they work for the people around them. Some of this reconnaissance may be automated using bots and crawlers to gather and validate information.

Why is CEO Fraud a whole-of-business risk?

CEO Fraud is not an isolated IT issue—it's a serious threat to business viability. CEO Fraud can have wide-ranging impacts from monetary losses to ruined careers, lowered share prices and reputational damage for the company and individuals involved. Company boards or shareholders may not excuse financial losses from CEO Fraud, so the responsibility for better security practices must be taken seriously by management at all levels.

> "CEO Fraud is a serious threat on a global scale. It's a prime example of organised crime groups engaging in large-scale, computer-enabled fraud, and the losses are staggering."
>
> ***—Maxwell Marker, FBI Special Agent, Criminal Investigative Division***

It only takes a second to lose millions

Large-scale company data breaches

No business is immune to email fraud attacks. Technology giants Facebook and Google were victims of socially engineered email fraud attack over two years, siphoning USD$100 million to various Eastern European bank accounts. The Lithuanian perpetrator impersonated a large, Asian-based computer manufacturer—a regular supplier to both companies—by falsifying email addresses, invoices and corporate stamps.

In what has been one of the largest data breaches yet seen, Equifax admitted in September 2017 that hackers stole the personally identifiable information of up to 143 million US consumers. Equifax share values plummeted by one third, a week following the public announcement. The CEO, CIO and CSO all exited the company less than a month later and were scrutinised in a Federal Trade Commission investigation.

Why is CEO Fraud skyrocketing?

CEO Fraud is up 2370% since 2015

According to FBI data, CEO Fraud is responsible for over US$12.5 billion of business losses globally.

Australian Cyber Security Centre's Threat Report states that Australian businesses lost more than $20 million to CEO Fraud between 2016 and 2017.

CEO Fraud is the most prevalent type of phishing attack after Ransomware. Cyber perpetrators are resorting to socially-engineered attacks because the risk-to-reward ratio is huge. Common victims are those who have financial authority.

The most common CEO Fraud scenarios

Fake invoices from existing suppliers

Invoices sent from contractors, suppliers or other external parties that seem to have a legitimate relationship with the company.

Requests for personal data

Requests for confidential or personal information, often from either a person of authority or the company's legal counsel.

Urgent funds transfer requests

Urgent request for a transfer of funds from a person of authority within the organisation. Usually sent as a plain text email without email signatures and other corporate branding.

Availability and location requests

Checking to see if a person is available or on location. Often this type of fraudulent email is for reconnaissance purposes and precedes the actual attack.

Why traditional antivirus solutions struggle to stop CEO Fraud

Traditional antivirus solutions look for the presence of a cyber threat in the form of a link, file attachment or unusual activity such as a bulk email run. In CEO Fraud emails, none of those threat indicators are present.

CEO Fraud emails look just like the thousands of plain text messages passed through antivirus every day/products every day. They are directly addressed to unsuspecting employees who believe they are legitimate emails from a person of authority within the company. Every CEO Fraud situation is unique, and different individuals can be the target of extremely personalised and relevant messages.

What you can do to protect your business?

Board and C-level business governance around cybersecurity and cyber threats is vital. Cybercrime is no longer just an IT department issue—top-down leadership is key in protecting business assets and reputation.

If your company is receiving unwanted email, you are at risk

Executives need to be prepared. Start conversations now with your board members, C-level colleagues and IT managers about what measures you have in place to deter criminal-intent email.

6 WAYS TO PROTECT YOUR COMPANY FROM CEO FRAUD

1

USE A CLOUD-BASED EMAIL AND WEB SECURITY SERVICE

Services such as MailGuard can predict and prevent criminal-intent email threats in real-time

2

BACKUP YOUR DATA

Secure your files and data with a cloud-based backup

3

PREVENT FRAUDULENT PAYMENTS

Implement tight internal third-party payment policies and processes

4

STAY UP-TO-DATE

Ensure all hardware touch-points to the internet are using up-to-date virus protection

5

UPDATE YOUR POLICIES

Implement a robust cybersecurity policy that all employees understand

6

GET INSURED

Get comprehensive cybersecurity insurance that covers your company's specific circumstances

About MailGuard

Email security experts since 2001

MailGuard is a world-class, advanced email security solution that detects and blocks fast-breaking zero-day email threats 2 to 48 hours ahead of the market.

With proprietary Hybrid Artificial Intelligence (AI) threat-detection engines, MailGuard predicts, anticipates and learns about new and emerging threats, so your company is protected from the moment of attack.

MailGuard works seamlessly alongside Office 365 and Microsoft's native security offerings such as Exchange Online Protection and Advanced Threat Protection. We share threat intelligence and collaborate closely with Microsoft teams to deliver multi-layered defence for business.

MailGuard is a certified Microsoft Gold Partner

Gold
Microsoft Partner