mailguard

What every executive needs to know about targeted CEO fraud

What is CEO fraud?

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

Whaling 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 and those around them. Some of this reconnaissance may be automated using bots and crawlers to gather and validate information.

Cyber-perpetrators regularly check company websites, social media postings and profiles, and scan industry news for upcoming events, important projects, company mergers or acquisitions. When the timing is right, they pounce with targeted, plain-text emails: personalised communications with minimal or no text formatting or design.

Why Is this 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, lower share prices and reputational damage for the company and individuals involved. Financial losses from CEO fraud may not be excused by company boards or shareholders, so the responsibility for better security practices must be taken seriously by management at all levels.

"BEC (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

No business is immune to fraudulent attacks. Technology giants Facebook and Google were victims of socially engineered email fraud attack over a two-year period, 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.

Who takes the blame?

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 sky rocketing?

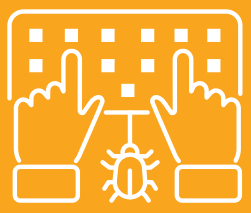
According to FBI data, CEO fraud has shot up by 2,370% since January 2015, resulting in reported exposed losses of over USD$5.3 billion globally. CEO Fraud is the most prevalent type of phishing attack after ransomware.

Cyber perpetrators are resorting to sociallyengineered attacks because the risk-to-reward ratio is huge. Common victims are those who have financial authority.

An FBI analyst has reported that the average financial loss to individuals is USD$6,000; an organisation USD$130,000. These are attractive windfalls for criminals.

The most common CEO fraud scenarios

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



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

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

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

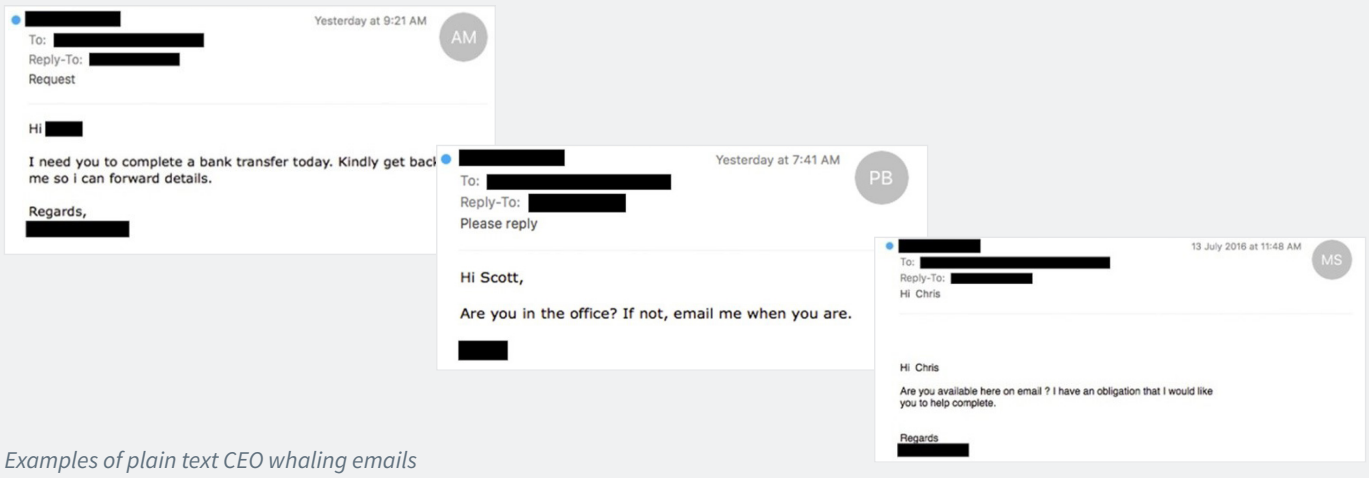
Why traditional antivirus solutions struggle to stop CEO fraud

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 AV products every day. They are directly addressed to unsuspecting employees who believe they are legitimate emails from a person of authority in their business. Every CEO fraud situation is unique, involving different individuals being targeted with 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.



Examples of plain text CEO whaling emails

Six cybersecurity musts for companies

1. Use a cloud-based email and web security service such as MailGuard that can predict and prevent criminal-intent email threats
2. Secure your files and data with a cloud-based backup
3. Prevent fraudulent payments by implementing tight internal third-party payment policies and processes
4. Ensure all hardware touch-points to the internet are using up-to-date virus protection
5. Implement a robust cybersecurity policy that all employees understand
6. Get comprehensive cybersecurity insurance that covers your company's specific circumstances

About MailGuard

- MailGuard detect and block fast-breaking, criminal intent email threats 2-48 hours ahead of the market.
- Our hybrid Artificial Intelligence (AI) engines predict, learn and anticipate new threats as they begin circulating. This means your company is protected from new threats and their variants from the moment of attack—from 'day zero'.
- We've developed sophisticated proprietary cybersecurity intellectual property (IP) with 17 years experience profiling both legitimate and unwanted email to stop fraud.
- The MailGuard team tests emails, in near real-time, checking tens of thousands attributes to ensure nothing malicious gets through.
- MailGuard works seamlessly alongside Office 365 and Microsoft's native security offerings such as Exchange Online Protection and Advanced Threat Protection. We share intelligence threats and collaborate with the Microsoft 365 team for product development.

Cybercriminals move at a rapid pace: every minute matters

Discover how simple and effective it is to protect your organisation from threats such as CEO fraud. Get a free 14-day MailGuard trial today: bit.ly/mailguard-trial

Contact a MailGuard consultant
Phone 1300 30 44 30
Email expert@MailGuard.com.au

www.mailguard.com.au

mailguard