CSIS

REST ASSURED.

Email Fraud Protection

MINIMISE FRAUDULENT PAYMENTS

www.csisgroup.com

EMAIL FRAUD. THE NUMBERS

08% **Businesses** admitting they have been targeted by impersonation fraud.

06% **Businesses** where jobs have been lost due to the financial impact of email fraud.

07% **Businesses** that have experienced financial hardship due to email fraud.

58% **Businesses** reporting a rise in email fraud. Unreported crimes push the real figure even higher.

EMAIL FRAUD. THE POTENTIAL IMPACT

Immediate

Largely unavoidable costs that include the immediate business and media impact, plus the cost of restoring the confidentiality, integrity and availability of data and systems.

- Forensic investigation
- Customer notification
- Legal costs
- Business interruption
- Public relations and crisis management
- Fraud / extortion
- IT / business remediation

Slow burn

Typically include the long-term business impact and costs incurred by reimbursement, reparation and financial penalties for failure to meet obligations.

- Loss of revenue
- Loss of management focus
- Negative share price
- Third-party litigation
- Damaged brand reputation
- Customer churn
- Loss of competitive advantage

THE MOST COMMON EMAIL SCAMS

CEO/CFO/Executive fraud

After breaching an executive's email account, the criminal often waits until the executive is on holiday or travelling abroad, and therefore not easily reached quickly. The criminal then sends a plausible-looking email to a junior member of staff requesting an urgent transfer of funds. Pressurised to make the payment without following due process, the staff member transfers the money into a criminal bank account.

Invoice fraud

The criminal impersonate a genuine supplier and requests that bank account details are changed, diverting payment for goods or services into their own bank account. The criminal will usually spend time discovering when regular payments are made, and then contacts the company explaining a change of bank account details. This type of fraud can remain undetected for weeks until the genuine supplier chases a payment, by which time the money trail has gone cold.

Business email compromise (BEC)

After compromising an email account, the criminal changes the beneficiary details so that payments land in a criminal account. The criminal then sends an email from an executive's account authorising a payment.

Often embedded in a genuine email chain (where authentication may already have occurred), the payment is made in good faith to the account details provided. Both parties usually remain unaware of the crime until the payment is queried.

Payroll diversion

A high-loss crime using phishing emails to capture employee login credentials. Once logged into the account, the criminal changes direct deposit information to redirect payroll into their own account. The FBI have noted that despite the relatively low number of complaints they receive about this type of crime, the average reported loss for each incident is around $1 million.

Email Fraud Protection (EFP) provides fast detection and remediation in case of fraud attempts via email.

The software

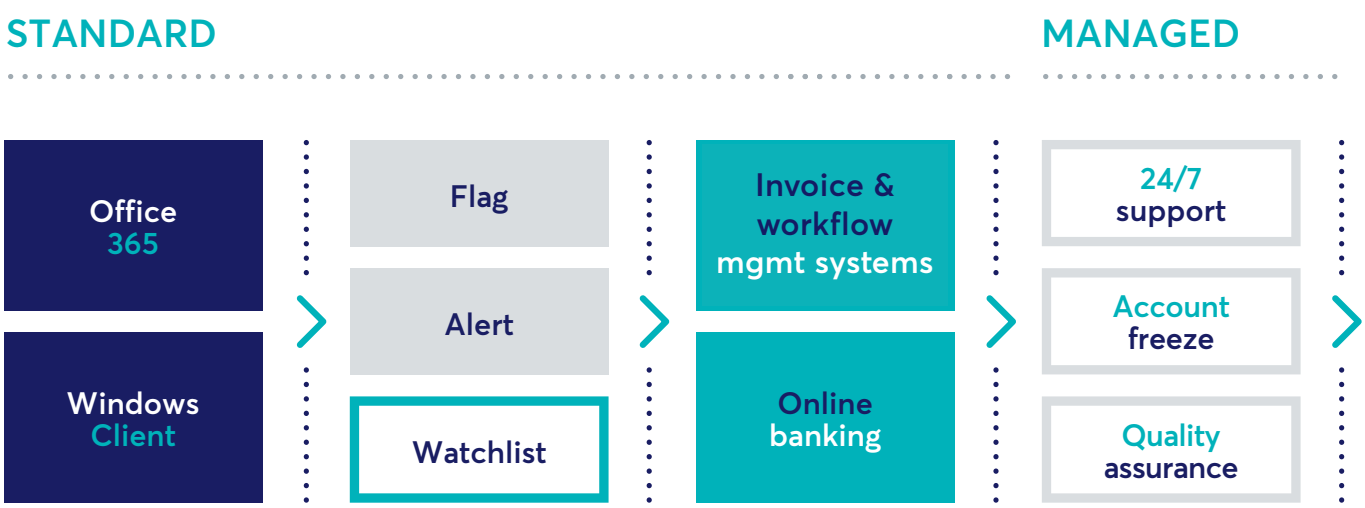
The software (available for endpoint installation or as a cloud-based app) provides an added security layer to existing email security and internal control systems. The software monitors and analyses all incoming and outgoing emails for fake invoices, fake bank account updates, malware attachments, and phishing URLs.

Unlike traditional email fraud software, EFP is able to continuously monitor the emails received and reacts in real time or historically. The software uses a unique algorithm to develop continuously while processing further data. The software is built by fraud specialists in close collaboration with banks and CFOs.

Product options

SOFTWARE	**IMPLEMENTATIONS**	**Cloud** Office 365	**On premise** Windows Client
	INTEGRATIONS	**Invoice & workflow mgmt systems + Online banking**	
MANAGED	**SERVICES**	**24/7 fraud specialists support**	

How it works



01

Implementations

Email Fraud Protection is easily installed by the customer, either as an Office 365 cloud app for the entire organisation or as an Windows client for individual users.

02

Handling

All inbound and outbound emails are monitored for financial content. Any financial related emails are flagged and assessed for their risk level. Suspicious emails are detected and key employees alerted. Non-suspicious emails are delivered and put on a watchlist for continuously monitoring.

03

Integrations

The system integrates to online banking and selected payment control systems. Provides users with alerts in familiar systems.

04 (optional)

Services

CSIS Managed Services ensures 24/7 support and quality assurance on every alert. Our long-lasting relationships within the financial sector and law enforcement allows us to rapidly freeze accounts and retrieve stolen money after fraudulent money transfer attempts. The risk is significantly reduced if the email fraud is found within the first 24 hours.

Windows client minimum requirements:

Net version 4.6.1 or newer / Windows 7 (32/64 bit) SP1 or newer.

Monitor and analyse all emails for fake invoices and fake bank account updates.

Benefits

- Add an extra security layer to any existing email security product.
- Rate every invoice for authenticity or indicators of compromise.
- Monitor compromised emails from vendors, suppliers and internal accounts.
- Detect fake invoices, even from compromised email accounts.
- Detect advanced phishing and malware emails.
- Continuously scan emails, including archived content and attachments.
- Easy integration with payment control systems.
- Rapid account and money transfer freezing.

Features

- Integration to email cloud providers such as MS Office 365.
- Easy implementation on Office 365 or client-side.
- Software can run both server and client side.
- Threat intelligence feed focused on financial threats.
- Money transfer freezing.
- Historical alerting.
- Risk assessment and mitigation managed by 24/7 fraud security specialists.

Add a robust security layer to your existing payment procedures.

Learn more

For more information, please see **www.csisgroup.com**

REST ASSURED.

CSIS IN BRIEF

- Founded in Copenhagen in 2003.
- Preferred IT security provider to some of the world's largest financial services and enterprise organisations.
- Trusted adviser to regional, national and international law enforcement agencies.
- Credited by Gartner Group for outstanding threat intelligence capabilities.
- Renowned for cybersecurity advisory services and managed security solutions, as well as incident response, forensics and malware reverse engineering capabilities.

CSIS Security Group A/S

Head office
Vestergade 2B, 4th floor
1456 Copenhagen
Denmark

UK office
95 Aldwych
London, WC2B 4JF
UK

+45 88 13 60 30
contact@csisgroup.com

www.csisgroup.com