Standard Chartered

Do you see what we see? Business Email Compromise

Business email compromise (BEC), uses phishing tactics to deceive recipients.

US$26 billion

was lost to phishing between 2016 and 2019[1].

The number of BEC attempts — also known as

CEO FRAUD or **WHALING**

1. increased by — **100%** between May 2018 and July 2019[1]
2. have been reported in — **177 countries**[1]
3. reached an average daily volume of — **128,700** from January to March 2019[2]

The top 10 countries targeted by BEC fraudsters (July 2018–June 2019)[2]

1. United States
2. United Kingdom
3. Australia
4. Belgium
5. Germany
6. Canada
7. The Netherlands
8. Hong Kong
9. Singapore
10. Japan

Top keywords used in emails to catch recipients off guard (July 2018–June 2019)[2]

- Transaction request
- Outstanding payment
- Important
- Important update
- Urgent
- Attention
- Request
- Payment

Close to **30%** of targeted BEC attempts were directed at generic email accounts, such as "sales@company.com"[3]

About **43%** of BEC scams impersonate **CEOs or founders**[4]

Nearly **47%** of BEC scams try to deceive the recipient into making a **wire transfer**[4]

Don't rely solely on software to keep you safe!

25% of phishing emails are undetected by Office 365's default security features[5].

50% of all phishing emails are believed to contain malware which is designed to damage computers with spyware and viruses[5].

Fraud can be hard to spot at times, but together, we can reduce the risk by following these simple steps.

SPOT THE WARNING SIGNS

Always check that the email address is spelt correctly, or hover your mouse over the email address to see the domain URL.

STOP SUSPICIOUS ACTIVITY

Never release any funds without verifying with the recipient. The best way to do this is to call them, but do not call using the number on the email.

REPORT THE INCIDENT

If you suspect any fraud activity, report the incident to the bank or to your local authorities immediately. The quicker the fraud is reported, the higher the chances of recovery.

SPOT. STOP. REPORT

Sources: 1. Federal Bureau of Investigation, Business Email Compromise the $26 Billion Scam, 2019. 2. Symantec, BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly, 2019. 3. Proofpoint, Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks, Winter 2019. 4. Barracuda Networks, Threat Spotlight: Barracuda Study of 3,000 Attacks Reveals BEC Targets Different Departments, 2018. 5. Avanan, 2019 Global Phish Report, 2019.