28 AUGUST 2020

WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

West Midlands | Regional Cyber Crime Unit

Business Email Compromise

Business email compromise (or BEC) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

What scammers might do:

- Spoof an email account or website. Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- Send spearphishing emails. These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- Use malware. Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

BEC Examples

- The Bogus Invoice Scheme: An attacker pretends to be the supplier and requests a funds transfer to an account the attacker controls. Companies with foreign suppliers are often targeted with this tactic.
- CEO Fraud: Attackers pose as an executive and send an email to employees in finance, requesting that they transfer money to a bogus account. Often requested as a matter of urgency and when the CEO may be otherwise engaged.
- Account Compromise: An executive's or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts.
- Impersonation: When a legal representative's e-mail address is used to contact clients, asking that they pay money to an account controlled by the attacker.
- Data Theft: Employees are targeted to obtain Personally Identifiable Information (PII) of employees and executives. Such data can then be used for future attacks.

Why BEC scams are effective?

- An attacker will conduct research when targeting a company executive or employee (social media, LinkedIn, Companies House, accounts and website). This research makes the email more convincing to the recipient.
- The email contains no hyperlinks or malware attachments, which is usually identified and removed by traditional IT security systems.
- An attacker will spoof an organisation's name. For example, instead of using johnsmith@trident.com, they will use johnsmith@tridant.com – it can be hard to spot the difference.
- An attacker may monitor corporate communications to identify the best tactics and timing to employ for a successful attack.

Mitigation Advice

- Training: Train staff to identify fake emails. Always be sceptical of urgent and hurried requests to transfer money. Verify those requests either by phone or in person.
- 2-Step Factor Authentication (2FA): 2FA will protect user accounts from being hijacked by an attacker. Usernames and passwords require us to 'know something' and we can prove who we are by 'having something', such as a pin sent to our phone.
- DMARC: This enables an organisation to verify that an email they receive aligns with what they know about the sender. The technology is extremely effective in eliminating spoofed emails. See here for more information
- Secure Email Gateway: This is your email 'firewall'. It will stop spam, malware and viruses, but it can also be configured to hunt for key words such as 'payment', 'urgent', 'sensitive' and 'secret'.
- Add Warning Banners: Most email systems can be configured to place warning banners on emails from new or unusual contacts, helping to mitigate the risk of lookalike domain spoofing.
- Visit the NCSC BEC Infographic at https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf