# Ways to Mitigate Business Email Compromise

Author: eFraudPrevention

BankUnited

Business Email Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

## Non-Technical Mitigations

### Social Engineering Safety

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Be careful what you post to business networking sites like LinkedIn and your company website, especially information about who has which specific job duties.

### Training and Awareness

- Alerts for employees and customers regarding phishing scams targeting specific organizations or interest groups.
- General information on phishing tactics posted to an organization web site or emails.
- Establish an employee testing program with phishing and BEC attempts that appear to come from your senior leaders and trusted business partners.

### Standardize Validation for Payments and Account Changes

- Establish with your customers and business partners how changes in account information will be communicated and validated.  Also, confirm how you expect them to validate changes to your banking information.

### Confirm Significant or Out-of-Pattern Changes

- Beware of sudden changes in business practices. For example, if a vendor suddenly asks to be contacted at a personal email address when all previous official correspondence has been on a company email, verify via other channels that you are still communicating with your legitimate business partner.
- Be especially wary if the requestor is pressing you to act quickly.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in an account number or payment procedures with the person making the request.
- Watch for suspicious requests, such as a change in a vendor's payment location.
- Follow controls for the validation of new or revised payment information.
- Escalate any concerns if a payment seems suspicious - even after performing a callback.
- Be very suspicious if a vendor offers vague reasons for changes to a new account, such as tax audits or current events, e.g., "Due to COVID-19, we need to update our payment information…"

### Create a Social Media Policy

- Construct, implement and enforce a social media policy that prohibits sharing details about company roles and responsibilities, so cyber criminals cannot develop a picture of your corporate structure, including addresses to target your employees.

## Email

- Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing). Look up the number from an external source when calling and call the company to ask if the request is legitimate.
- Check the “rules” setting on your account periodically to ensure that no one has set up auto-forwarding for your e-mails.
- Email forwarding vs email reply. Instead of hitting reply on important emails, use the forward option and either type in the correct email address or select it from your email address book to ensure you’re using the real email address.
- Be cautious about using out-of-office replies that give too much detail about when your executives are out of the mix.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don’t know and be wary of email attachments forwarded to you.
- Avoid clicking on links or attachments from unknown senders. Doing so could download malware onto your company’s computers, making you vulnerable to a hack.

## Anti-Phishing Strategies for AI-Written Emails

- Sandboxing for Word documents and other attachments to keep them away from corporate networks.
- Web traffic inspection through a secure web gateway to protect both on-prem and remote users.
- Check URLs for malicious content or typo squatting.
- Deploy email security protocols such as DMARC, DKIM, and SPF, which help prevent domain spoofing and content tampering.
- Provide an easy way to report suspicious emails.

## Technical Mitigations

- Set up two-factor (TFA) or multi-factor authentication (MFA) on any account that allows it, and never disable it. TFA/MFA aims to protect users if authentication credentials have been captured. The nature of changing tokens limits the attacker’s ability to leverage captured credentials.
- Avoid free web-based e-mail accounts. Establish a company domain name and use it to create formal e-mail addresses for your employees.
- Label external emails to help prevent the impersonation of employees.
- Ensure emails originating from outside the organization are automatically marked before received.
- Prohibit automatic forwarding of emails to external addresses. Detect email inbox forwarding rules that send all or selected emails to an external email address.
- Add an email banner to messages coming from outside your organization. This is a simple way to highlight that extra scrutiny is needed for external emails. It can also identify when an adversary creates a fraudulent domain that looks similar to a healthcare and public health sector (HPH) legitimate domain.
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Enable alerts for suspicious activity, such as foreign logins.
- Enable security features that block malicious emails, such as anti-phishing and anti-spoofing policies.
- Configure Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate email.
- Disable legacy account authentication.

- Apply patches/updates immediately after release/testing; develop/maintain patching program if necessary.
- Implement an Intrusion Detection System (IDS); keep signatures and rules updated.
- Implement spam filters at the email gateways; keep signatures and rules updated.
- Block suspicious IP addresses at the firewall; keep firewall rules updated.
- Implement whitelisting technology to ensure that only authorized software is allowed to execute.
- Implement access control based on the principle of least privilege.
- Implement and maintain anti-malware solutions.
- Conduct system hardening to ensure proper configurations.
- Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.
- Domain-based Message Authentication Reporting and Conformance (DMARC). The DMARC protocol enables domain owners to specify which authentication method is used when sending emails. DMARC helps email receivers determine if the purported message "aligns" with what the receiver knows about the sender. If not, guidance is provided on how to handle the message.
- Protect your web domain. Consider hiring a firm that will notify you of web domains that have been registered to deceptively look like your own; cybercriminals can use lookalike domains in BEC attacks to trick your employees or business partners into diverting funds.
- Data Mining. Data mining abuse box/phishing reporting and using the intelligence gained to prevent future attacks.
- Passwords:
    - Review password policies to ensure they align with the latest NIST guidelines and deter the use of easy-to-guess passwords.
    - Review IT Helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts.
    - Regularly audit user passwords against common password lists, using free or commercial tools.
    - Provide pragmatic advice to users on how to choose good passwords.

### Proper Callback Procedures

An appropriate process requires an employee, typically a payments staff member, to pick up the phone and validate new payment requests, requests to establish a new bank account, changes to payment instructions, and changes to contact information.

- Callbacks should be made to the actual person making the request using a phone number retrieved from a system of record when setting up a new account, processing a request for payment, changing payment instructions, or changing contact information. Be wary of vendors who frequently change payment instructions. Fraudsters will sometimes provide several different accounts to victims during a BEC fraud attempt. Confirm all of the account details, including the new account number.
- Do not confirm payment instructions only via email. Always perform a call back using a phone number from a system of record to the person making the request.
- If a callback is not currently a part of your company's payment control process, try to implement one or escalate the issue to someone who can.
- If you receive a call from your financial institution asking you to validate an unusual payment, take it seriously. It could be your last chance to stop a fraudulent payment before it's too late. Double-check that your controls have been properly executed. Do not assume a callback has been performed. Pay close attention to the information provided and reconfirm that your organization performed all applicable controls, including a callback. It is common to confirm payments as valid only to later report them as fraudulent.

- Understand that once a payment has been released, there are no guarantees the funds will be recovered.
- Keep your contact information up-to-date if your financial institution needs to reach you.
- Do not trust payment instructions provided by a business partner. Always validate that whoever is providing the instructions has performed a separate validating callback to the actual requestor.

*All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.*