INDEPENDENT FINANCIAL

BUSINESS EMAIL COMPROMISE FACTSHEET

WHAT IS BUSINESS EMAIL COMPROMISE?

Business Email Compromise (BEC) — also known as Email Account Compromise (EAC) — is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business — both personal and professional.

In a BEC scam, criminals send an email that appears to come from a known source making a legitimate request. For example:

- A trusted vendor sharing a link to download payment information, invoices, or work agreements.
- A financial document detailing unexpected payments with instructions on how to contest the transaction.
- A lending company providing borrowers instructions on how to update payment information or wire funds.

HOW CRIMINALS CARRY OUT BEC SCAMS

A scammer might:

- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@company.com vs. john.kelley@company.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.

HOW TO PROTECT YOURSELF

- **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.
- **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), and call the company to ask if the request is legitimate.
- **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.
- **Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.**
- **Verify payment and purchase requests in person if possible or call the person to make sure it is valid.** You should verify any change in account number or payment procedures with the person making the request.
- **Be especially wary if the requestor is pressing you to act quickly.**

WHAT YOU SHOULD DO

- Contact the organization being spoofed and notify them that their organization is being used in a BEC scam.
- Inform your coworkers and employees to raise awareness of the scam in case they receive similar emails.
- Contact your financial institution immediately to notify them of the scam and to monitor for suspicious activity.
- Report the scam to local law enforcement, the FBI's Internet Complaint Crimes Center at IC3.gov, and the FTC at ReportFraud.ftc.gov.

If you have any additional questions or would like additional information on cybercrime, please contact the Independent Financial Information Security Team at InfoSec@ifinancial.com.