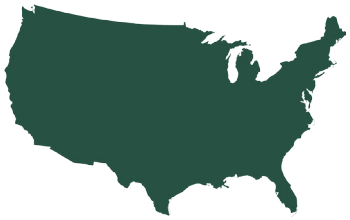
NACHA
The Electronic Payments Association

PROTECTING AGAINST FRAUD

How to spot and prevent fraud schemes

Fraud schemes continue to grow, evolve and target legitimate businesses, nonprofits, government and other public-sector organizations. Business Email Compromise and Vendor Impersonation Fraud are monitored by the FBI.



These scams have been reported in all 50 states and in 131 countries.[1]

Victim complaints filed with the Internet Crime Complaint Center and financial sources indicate fraudulent transfers have been sent to 103 countries.[2]

Since January 2015, there has been a 1,300 percent increase in identified exposed losses, totaling over $3 billion.[3]

1. https://www.ic3.gov/media/2017/170504.aspx
2. FBI's Internet Crime Complaint Center www.ic3.gov
3. https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

BUSINESS EMAIL COMPROMISE

What Is It?

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business' officers and monitor his or her account for patterns, contacts and information. Using information gained from social media or 'out of office' messages, the fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions.

How It's Done

STEP ONE

Fraudster monitors officer's accounts for patterns, contacts and information.

STEP TWO

After identifying the target, ploys are conducted such as spear-phishing, social engineering, identity theft, email spoofing, and the use of malware to either gain access to or convincingly impersonate the email account.

STEP THREE

Fraudster uses the compromised email account to send payment instructions.

STEP FOUR

Payment instructions direct the funds to an account controlled by the fraudster.

BUSINESS EMAIL COMPROMISE

Avoid Being a Victim

Solid internal controls are key to guarding against these scams.

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume it's a cybersecurity problem.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, or pressure to take action quickly.
- Authenticate requests to make payment or change payment information.
- Review accounts frequently.
- Initiate payments using dual controls.
- Never provide password, username, authentication credentials, or account information when contacted.
- Don't provide nonpublic business information on social media.
- Avoid free web-based email accounts for business purposes. A company domain should always be used to establish company personnel emails.
- To make impersonation harder, consider registering domains that closely resemble the company's actual domain.
- Do not use the 'reply' option when authenticating emails for payment requests. Instead, use the 'forward' option and type in the correct email address or select from a known address book.

"THE BEST WAY TO AVOID BEING EXPLOITED IS TO VERIFY THE AUTHENTICITY OF REQUESTS TO SEND MONEY BY WALKING INTO THE CEO'S OFFICE OR SPEAKING TO HIM OR HER DIRECTLY ON THE PHONE," SAID SPECIAL AGENT MARTIN LICCIARDO. "DON'T RELY ON EMAIL ALONE."[4]

4. https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

VENDOR IMPERSONATION FRAUD

What Is It?

Vendor Impersonation Fraud can occur when a business, public-sector agency or entity, such as a municipal government agency or a public university/college, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment along with routing and account information. This type of request could come from fraudsters and not the contractor. Although any business entity could be the target of this type of social engineering attack, public-sector entities seem to be specifically targeted because their contracting information is oftentimes a matter of public record.

How It's Done

STEP ONE

Fraudster monitors a business, public-sector agency or entity for publicly available contracting or vendor information.

STEP TWO

Fraudster contacts the entity by posing as a legitimate vendor or contractor to request updates or changes to payment information to an account held by the fraudster. Contact is made via email, fax, phone, or online form submission.

STEP THREE

Fraudster uses the compromised email account to send payment instructions, resulting in funds being transferred into the fraudster's account.

VENDOR IMPERSONATION FRAUD

Avoid Being a Victim

Solid internal controls are key to guarding against these scams.

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume this is a cybersecurity issue.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, or pressure to take action quickly.
- Authenticate requests to make payment or change payment information using existing contact information.
- Review accounts frequently.
- Initiate payments using dual controls.
- Do not provide nonpublic business information on social media.
- Do not use the 'reply' option when authenticating emails for payment requests. Instead, use the 'forward' option and type in the correct email address or select from a known address book.
- Make vendor payment forms available only via secure means or to known entities.
- Require changes to payment account information be made or confirmed only by site administrators, and use methods like verification codes to existing contacts.
- Do not ignore calls from a financial institution questioning the legitimacy of a payment.

NACHA
The Electronic Payments Association®

PAYROLL IMPERSONATION FRAUD

What Is It?

Fraudsters target individual employees by directing the employees to update or confirm their payroll information via a fake payroll platform that spoofs their employer's actual payroll platform. In some cases, the fraudster may claim the employee must do one of these: view a confidential email from human resources or the payroll department, view changes to the employees account, or confirm that the account should not be deleted. In any case, when the employee logs in from a link or attachment in the email, the fraudsters then use the stolen employee credentials to change payment information in the real payroll platform.

How It's Done

STEP ONE

Fraudster targets an employee by sending a phishing email that impersonates the employee's human resources or payroll department, as well as the company's payroll platform. The email directs the employee to log in to confirm or update payroll information, including bank account information.

STEP TWO

Employee clicks the link or opens the attachment within the email and confirms or updates the payroll information.

STEP THREE

The fraudster then uses the stolen login credentials to change payment information to an account controlled by the fraudster.

PAYROLL IMPERSONATION FRAUD

Avoid Being a Victim

- Employers should alert employees to watch for phishing attacks and suspicious malware links.
- Employees should be directed to check the actual sender email address, rather than just looking at the subject line, to verify that the email came from their employer or payroll service provider.
- Employees should not reply to any suspicious email; instead have them forward the email to a company security contact.
- Employees should not enter their login credentials when clicking on a link or opening an attachment in an email.
- Employer self-service platforms should authenticate requests to change payment information using previously known contact information. For example, requiring users to enter a second password that is emailed to an existing email address, or to use a hard token code.
- Employer self-service platforms also should reauthenticate users accessing the system from unrecognized devices, using previously known contact information.
- Set up alerts on self-service platforms for administrators so that unusual activity may be caught before money is lost. Alerts may include when banking information is changed, and multiple changes that use the same new routing number or identical account numbers.
- Employers should consider validating employees' new Direct Deposit information by sending ACH prenotification transactions.