Cyber Fraud Risk Briefing:
Business Email Compromise

Office of Inspector General, Legal Services Corporation

June 21, 2023

Agenda

01. Business Email Compromise schemes explained.

02. Business processes targeted by BEC schemes.

03. Tactics used by cybercriminals to compromise emails.

04. Best practices for employee education and awareness, fiscal controls, email security, and network security.

05. Discuss two examples of BEC schemes.

06. Additional resources for grantees.

Business Email Compromise (BEC)

- BEC is a type of cybercrime where the cybercriminal **uses email** to trick an employee into sending money or divulging confidential grantee information such as grantee account information or Personally Identifiable Information (PII).
- BEC schemes aim to exploit vulnerable **business processes** that involve a financial transaction by compromising email accounts to deceive employees.
- Typically, the ultimate goal of a BEC scheme is to **divert funds** through a financial transaction such as a wire transfer or a gift card purchase.

Business Processes Targeted by BEC Schemes

Payroll Direct Deposit

Largest Grantee Loss: More than $12,000

Vendor Payments

Largest Grantee Loss: More than $40,000

Gift Cards

Largest Grantee Loss: Approximately $4,000

Grant Remittances

Largest Grantee Loss: Approximately $1.1 million

Communications with Financial Institutions

No Losses Reported to the OIG, to date

Other Business Processes Targeted by BEC Schemes

Lawyer Impersonation

In this type of BEC scheme, cybercriminals aim to target clients by impersonating their attorney/law firm.

Data Theft

Many BEC schemes start by targeting a company's administrative department in order to steal sensitive information such as internal forms, PII, etc.

False Invoice Scheme

A cybercriminal impersonates a legitimate vendor and emails a fake invoice that resembles a real one. The email request asks for a payment different from the norm.

Targeting EDs and CEOs

A cybercriminal impersonates a company's CEO or ED through email to another employee. The email is an urgent request for a money transfer such as a direct deposit changes or gift cards.

Tactics Used by Cybercriminals to Compromise Emails

INTRUSION

Intrusions occur when cybercriminals gain **unauthorized access** to a grantee network or an employee computer.

Intrusions allow cybercriminals to access company data and legitimate accounts such as an employee's email account.

Tactics Used by Cybercriminals to Compromise Emails

SOCIAL ENGINEERING

A **manipulation technique** that exploits human behavior and error in order to gain access to sensitive information.

Possible steps of social engineering: INVESTIGATION, INFILTRATE, EXPLOIT, DISENGAGE.

Types of social engineering: URGENCY, TRUST, HEIGHTENED EMOTION.

Administration

Lucy Kelson
Executive Director

June Carver
Human Resources

Melanie Corman
Executive Assistant

Polly St. Clair
Payroll

George Wade
Fiscal Director

Meryl Brooks
Accounts Payable

William Thacker
Executive Assistant

Rich Beck
Director of Operations

Tactics Used by Cybercriminals to Compromise Emails

EMAIL SPOOFING

Email address mimics or masquerades a legitimate/known address.

Example 1:

bsmith@lsc.gov vs. bsmith@lsc.com

doej@legal-services.com vs. doej@legalservices.com

Example 2:

Betty Smith (only name appears)

dholqng-kntuer@medrobaw.mi (appears when you hover over name)

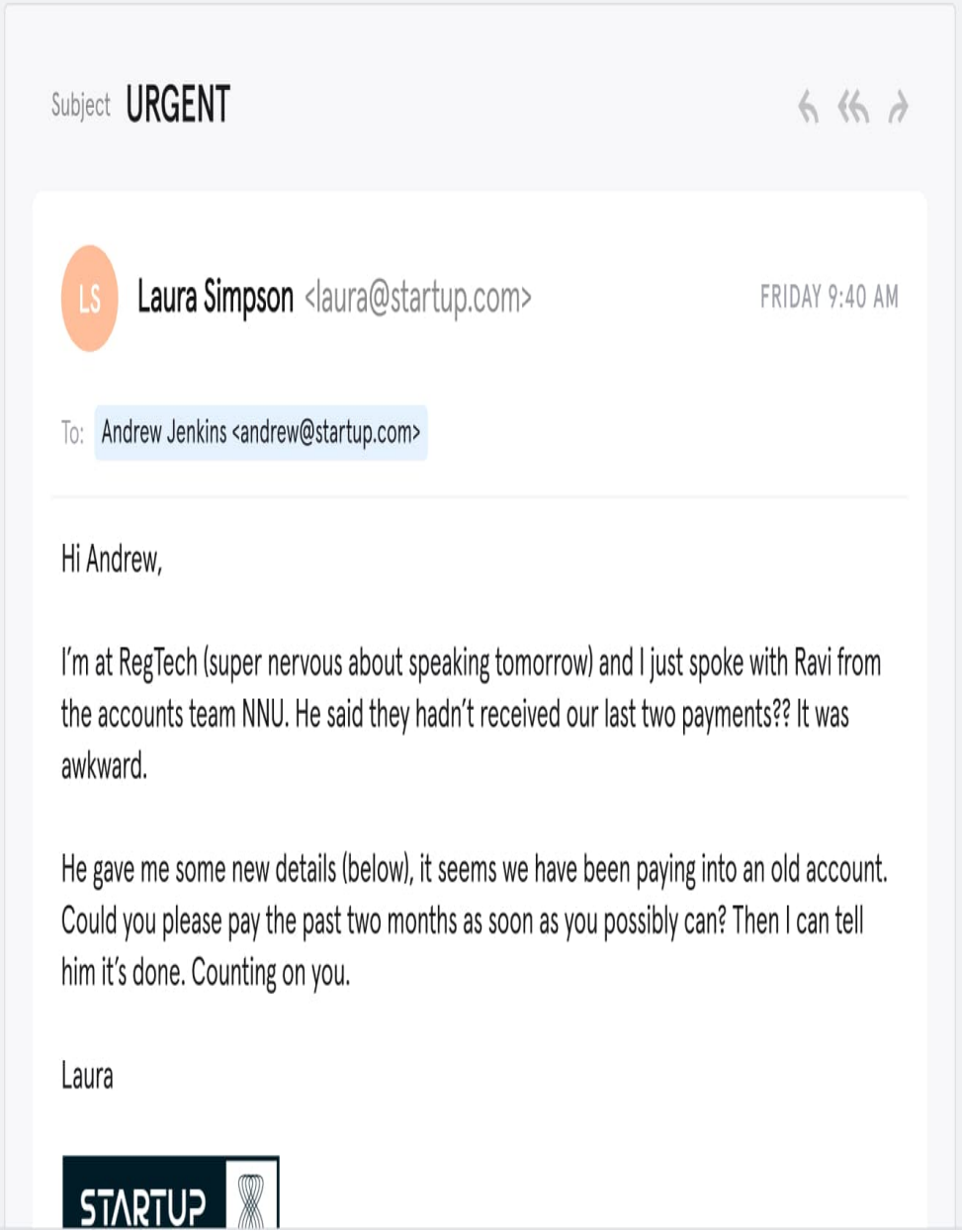
Tactics Used by Cybercriminals to Compromise Emails

SPEAR PHISHING

A type of email phishing attack that **targets a specific person or group** such as the finance department.

The emails typically have a personal tone and appear to be from a trusted sender.

Spear phishing can trick employees into making a transaction or disclosing sensitive information.



Best Practices:
Require Employee Education and Awareness

Require **cyberthreat training** for all staff especially HR, Accounting, and other Administrative staff.

Emphasize the **importance of cybersecurity** practices throughout the organization. Tone at the top matters.

Simulate BEC schemes for staff.

Have employees **report suspicious** emails and incidents.

Be wary of requests for information for items that should be common knowledge to the person requesting the information.

Prohibit personal emails or computers by staff for grantee-related activities.

Report cyber incidents to the OIG Hotline.

Cyber Humor: “Someone cracked my password. Now I need to rename my dog.”

Best Practices:
Implement Strong Financial Controls

Enable **automated notifications** for changes to automatic or recurring payments.

Verify the identity of the person/company requesting changes to payments or associated information.

Require at least **two-part authorization** (review and approval by more than one employee) for any requests related to changes in payments or money transfers.

Consider using a **system or software** specifically designed **to authenticate payments** rather than sending invoices through email.

Regularly **review and update financial policies** to ensure cybersecurity best practices and emerging threats are considered.

Follow written policies without deviation when dealing with requests related to financial transactions.

Best Practices:
Strengthen Email Security

Employ **multi-factor authentication** on grantee email accounts and other accounts such as payroll and billing software.

- A user would be required to present one or more verification factors in addition to their login credentials to gain access to the account or system.
- This additional measure helps prevent access when credentials are stolen.

Consider **blocking international IP addresses** from accessing your systems, especially email systems.

Implement **email authentication protocols** to help identify and block spoofed emails:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting, and Conformance (DMARC)

CYBER HUMOR: “What did the hacker's out of office message say? Gone phishing.”

Best Practices:

Implement Firewall Configuration and Software Patches and Updates

Ensure your network includes **a properly configured firewall** that only allows traffic needed for grantee operations.

- A firewall is a network security device that monitors incoming and outgoing traffic and blocks certain traffic based on security rules.

Ensure that the organization's **software and systems are up to date** with security patches and updates.

- Cybercriminals can exploit vulnerabilities in outdated or unpatched software and gain unauthorized access to the grantee's network.

Regularly review and assess your organization's software inventory to ensure all **applications are current and adequately protected**.

Review the devices on the organization's network against the devices inventory to ensure **only registered devices are connected to the network**.

Example 1

Email Sent to Payroll Requesting Direct Deposit Change

Cybercriminal used a Gmail email account to impersonate an actual grantee employee. The email appeared to be from the employee's personal email. Email was directed to the payroll administrator by name and had a sense of urgency.

Payroll Sends Internal Form to the Cybercriminal

Payroll administrator believed request was legitimate and provided a direct deposit change form to the cybercriminal via the Gmail account.

Cybercriminal Returns Form with Voided Check

Cybercriminal returned the form to the payroll administrator from the Gmail account. The form included the other employee's actual name, home address, and SSN. It also included a voided check with employee's name but was from the cybercriminal's bank.

Payroll Changed Employee's Direct Deposit

Payroll administrator changed the employee's direct deposit information to the cybercriminal's bank. The grantee deposited the employee's payroll into the cybercriminal's account.

Example 2

Grantee CFO Communicates with Vendor CPA Firm

Grantee CFO communicated through email with an employee of their CPA firm. The communications were legitimate. The emails discussed the amount the grantee would owe related the grantee's annual financial statements.

CFO Receives Similar Email from a Cybercriminal

The same day the CFO received an email from a cybercriminal impersonating the same employee at the CPA firm. The email appeared to be sent from the CPA firm's email domain with a slight variation.

Cybercriminal Sends Invoice and Used CPA Firm's Letterhead

Cybercriminal's email included a fake invoice with the same amount discussed in the legitimate emails and also included instructions for the CFO to make a wire payment to the cybercriminal's bank account.

CFO Makes the Payment to the Cybercriminal

CFO believed the email was legitimate and made the payment to the cybercriminal's bank through a wire transfer.

Additional Resources

LSC-OIG Website: https://www.oig.lsc.gov/

- Hotline
- Cyber Security Resources

FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/

- File Complaints
- Cyber Alerts