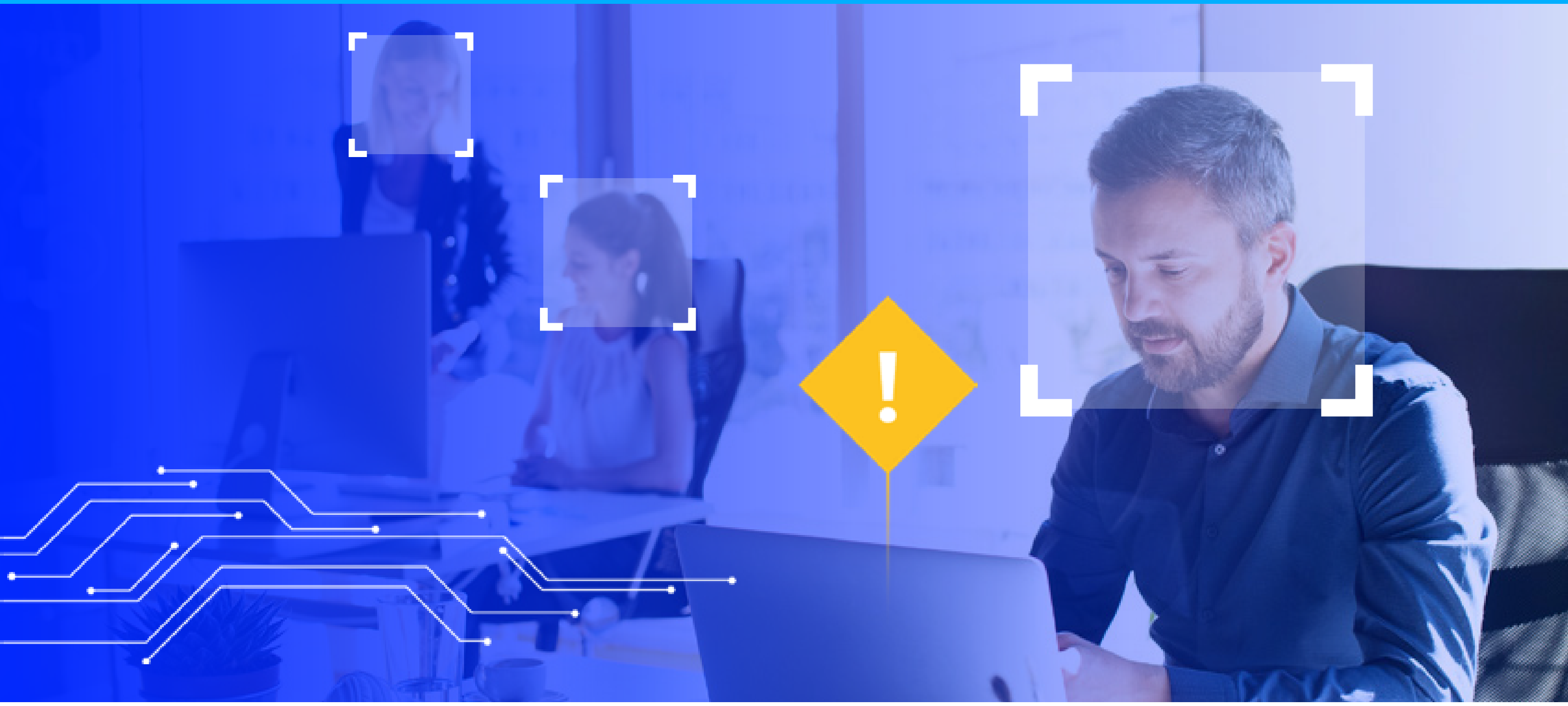
White Paper

Business Email Compromise (BEC) Attacks

IRONSCALES
SAFER TOGETHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS



Contents

IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

What is Business Email Compromise?

Business Email Compromise attacks are one of the biggest threats to every industry. BEC schemes cost an estimated $1.77 billion in 2019, and that number is only projected to skyrocket in the coming years. Whether you're in the commercial, government, and non-profit sector, you are at risk of BEC attacks.

BEC attackers use low-tech financial fraud that targets companies' sensitive data. They do not leverage malicious URLs or malware attachments. Therefore their attacks easily bypass signature-based prevention mechanisms used by Secure Email Gateways. And other legacy BEC safeguards – such as DMARC – are only effective against a small subset of phishing threats.

Breaking Down A Business Email Compromise Attack

Pretext

- Internal Employee
- Brand
- External Partner/Vendor

Approach

Impersonation

- Spoofing
- Look-alike Domains
- Display Name

Compromised Account

- Employee
- Partner/Vendor/Brand

Delivery

- Attachment
- URL
- Payload-less

Target

- Employee Inbox

IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

How Does Business Email Compromise Work?

Business Email Compromise attacks are one of the biggest threats to every industry. BEC schemes cost an estimated $1.77 billion in 2019, and that number is only projected to skyrocket in the coming years. Whether you're in the commercial, government, and non-profit sector, you are at risk of BEC attacks.

BEC attackers use low-tech financial fraud that targets companies' sensitive data. They do not leverage malicious URLs or malware attachments. Therefore their attacks easily bypass signature-based prevention mechanisms used by Secure Email Gateways. And other legacy BEC safeguards – such as DMARC – are only effective against a small subset of phishing threats.

A BEC attacker leverages social engineering tactics – typically accompanied by email spoofing or email compromise via phishing attacks or keystroke logging – to obtain employee credentials and access sensitive information.

While BEC attacks can involve many different vectors, they often start when an attacker sends an email to an employee with authorization to send wire transfer payments, requesting a change in business payment from the impersonated address of a supervisor, CEO, or trusted vendor.

Since the request comes from a seemingly trusted source, an employee will comply with the request. They don't realize that this request has given the attacker the upper hand and compromised their organization's safety.

Business Email Compromise attacks are one of the biggest threats to every industry. BEC schemes cost an estimated $1.77 billion in 2019, and that number is only projected to skyrocket in the coming years. Whether you're in the commercial, government, and non-profit sector, you are at risk of BEC attacks.

BEC attackers use low-tech financial fraud that targets companies' sensitive data. They do not leverage malicious URLs or malware attachments. Therefore their attacks easily bypass signature-based prevention mechanisms used by Secure Email Gateways. And other legacy BEC safeguards – such as DMARC – are only effective against a small subset of phishing threats.

Get Complete Mailbox BEC Protection From IRONSCALES

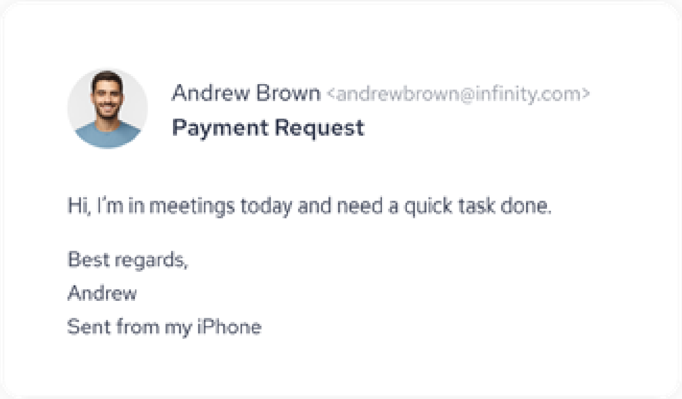
Types of BEC Attacks

There are many different types of BEC attacks. Since these scams do not always leverage traditional attack vectors like attachments or malicious links, they may evade identification safeguards.

Knowing what types of BEC attacks exist can help you from becoming a victim.

CEO Fraud

CEO fraud attacks involve impersonations of the CEO or other C-Suite executives. The attacker uses fraudulent credentials to direct employees in financial roles to transfer money to specific accounts.



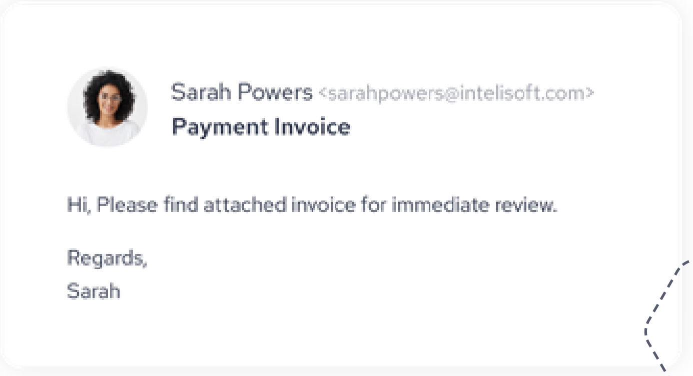
Andrew Brown <andrewbrown@infinity.com>
Payment Request

Hi, I'm in meetings today and need a quick task done.

Best regards,
Andrew
Sent from my iPhone

Account Takeover

Account takeover uses a trusted employee or executive's email account to solicit vendors for invoice payments with new bank account information. Then these invoice payments are deposited into criminal bank accounts.



Sarah Powers <sarahpowers@intelisoft.com>
Payment Invoice

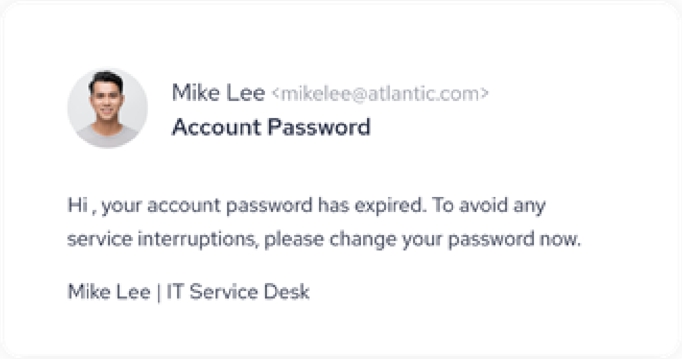
Hi, Please find attached invoice for immediate review.

Regards,
Sarah

Learn more about Account Takeover

Credential Theft

Credential theft attacks are often the catalyst to account takeover attacks. These attacks involve stealing a victim's proof of identity using phishing tools like fake login-pages or keystroke loggers. Once an attacker gains access to a victim's account privileges there is an open back door. They can sell those credentials on the dark web or use them to inflict massive financial and reputational damage to your organization.



Mike Lee <mikelee@atlantic.com>
Account Password

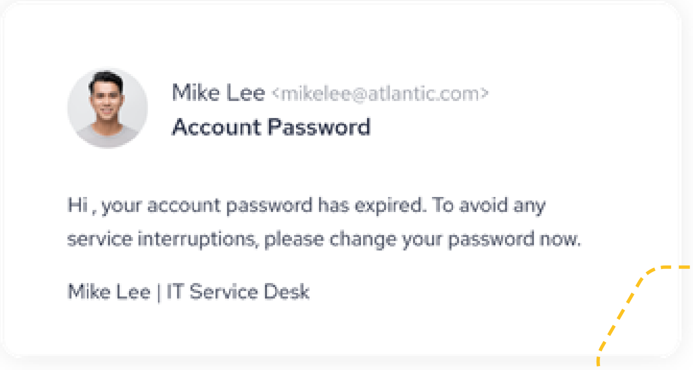
Hi , your account password has expired. To avoid any service interruptions, please change your password now.

Mike Lee | IT Service Desk

Invoice Fraud

Invoice attacks involve impersonation of an external partner/vendor, internal employee, or brand to deliver a fraudulent invoice request. Often the attacker requests fund transfers that unsuspecting employees deposited into criminal bank accounts. These requests don't contain malware, so they go undetected by SEGs.

Invoice attacks are costly, and they account for some of the most significant financial losses in BEC schemes.



Mike Lee <mikelee@atlantic.com>
Account Password

Hi , your account password has expired. To avoid any service interruptions, please change your password now.

Mike Lee | IT Service Desk

Common Business Email Compromise Methods & Tactics

Attackers utilize many different vectors to invade your network. Two of the most frequent are email impersonation and email spoofing.

Email Sender Impersonation

Email impersonation uses lookalike credentials of a specific person or entity to impersonate a known sender. Because lookalike credentials are visually similar to a targeted user, targeted brand, or targeted domain, many people cannot spot the discrepancy.

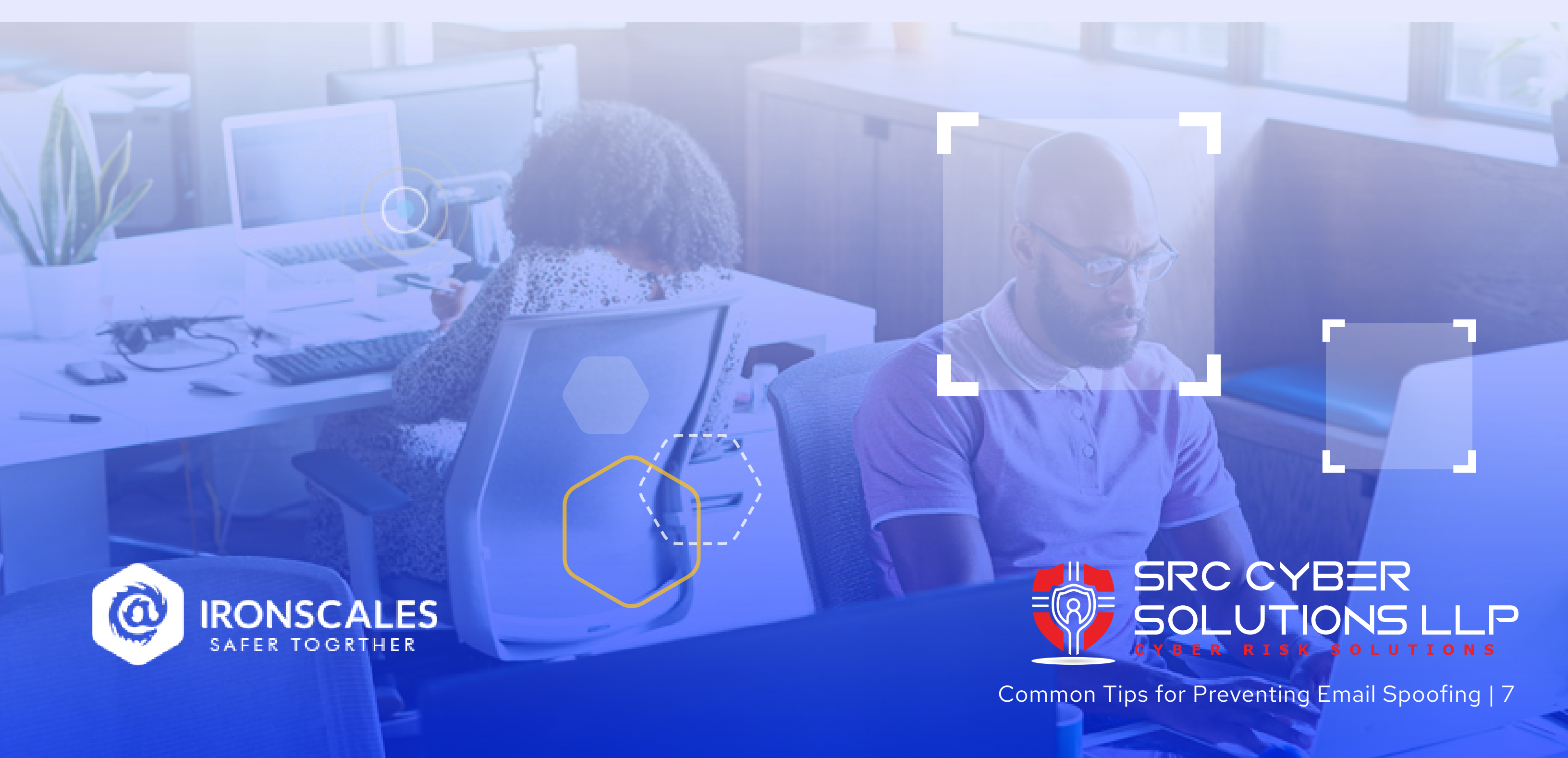
For example, the exact email address of **stevejobs@techcompany.com** might be impersonated with the similar looking **stevejabs@techcompany.com**

Email Spoofing

Email spoofing involves an attacker sending a message from -- or as a representative of -- an authenticated domain. These attacks may appear to come from legitimate addresses, but with slight variations that cloak the attacker. There are different types of email spoofing including lookalike/cousin domain, and exact domain.

For example, the exact email address of **stevejobs@techcompany.com,** might be spoofed with the lookalike/cousin domain **stevejobs@tecchcompany.com,** Or the attack could come from an exact domain spoof as **stevejobs@techcompany.com**

Learn More About Email Spoofing

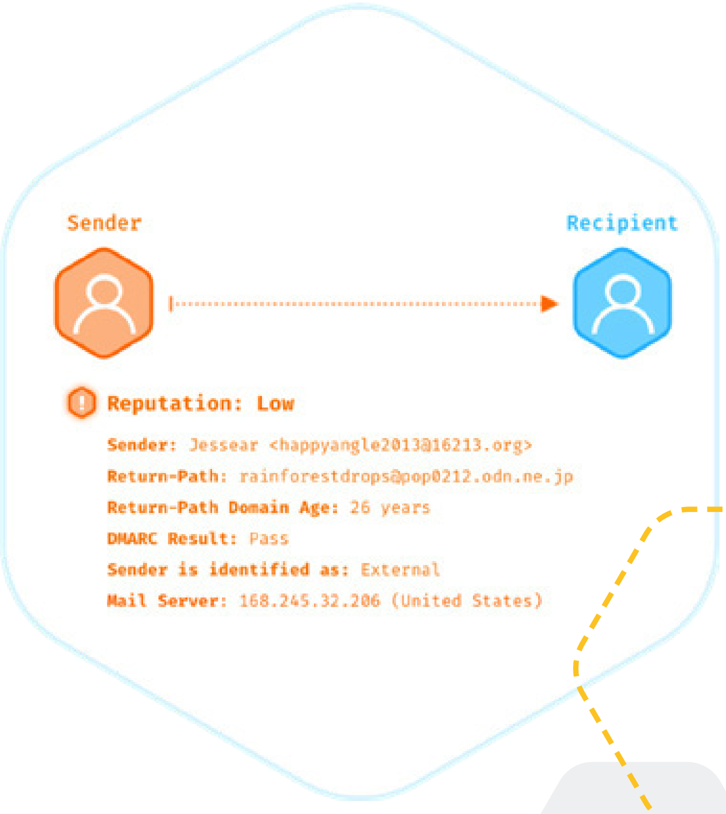


How To Stop Business Email Compromise Attacks

Email is an essential tool for any modern business. Preventing business email compromise attacks is a problem for all businesses. In the face of increasingly sophisticated email attacks, many organizations are looking for solutions for stopping BEC attacks. And many are struggling to find a truly comprehensive solution.

IRONSCALES comprehensive SaaS platform gives you an edge against all attackers with an inside out approach to email security. The IRONSCALES platform protects your organization from BEC attacks by analyzing all email communications and creating unique fingerprint profiles for each user. By cross-checking and verifying all incoming messages, IRONSCALES gives you confidence in a sender's identity while protecting your assets – all in real-time.

✓ Get Complete Mailbox BEC Protection from IRONSCALES



Reputation: Low

Sender: Jessear <happyangle2013@16213.org>
Return-Path: rainforestdrops@pop0212.odn.ne.jp
Return-Path Domain Age: 26 years
DMARC Result: Pass
Sender is identified as: External
Mail Server: 168.245.32.206 (United States)

Protect Yourself from Email Spoofing with IRONSCALES

IRONSCALES is a self-learning email security platform that can anticipate, identify, and react to targeted threats. Not only can the IRONSCALES platform help prevent email spoofing, its services reach beyond that to provide a secure and comprehensive experience for any company. Every time an email reaches your server, IRONSCALES looks for anomalies that could indicate impersonation, credential harvesting attempts, and known malware. IRONSCALES also has built-in natural language processing capabilities to pick up on fraud, and can cross-check emails against a log of emails other companies or employees have flagged.

With IRONSCALES advanced protection, you can avoid the adverse effects of spoofing and ensure a safe experience for employees and clients alike.

Learn more about what SRC Cyber Solution LLP has to offer by scheduling a demo today.

★★★★★

Great anti-phishing platform

-CISO in the Services Industry

Great anti-phishing platform that really gives added value for attacks a mail relay can't detect properly. Also help with forensic investigation of email incidents. Awareness program is nice and the reporting add-on can be implemented on many platforms (Outlook desktop/phone app, OWA).

Awards

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

www.srccybersolutions.com | +91 120 232 0960 / 1
sales@srccybersolutions.com

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email ecurity and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com