# SecurityAwarenessNews

the security awareness newsletter for security aware people

## CEO Fraud:
### Becoming the Boss

**Email Spoofing**

**Business Email Compromise**

**Zero Trust Security**

# EMAIL SPOOFING

## EXPLOITING YOUR INBOX

**Email spoofing is a technique used by cybercriminals to defraud people of information or money. It's a form of forgery that exploits the standard protocol for sending emails so they appear to come from someone you know and trust. There are a few ways to do this.**

One is to change the display name (the "From") of the sender to mimic someone else. For example, you could get an email that appears to come from a co-worker. Upon inspecting the message, however, you should notice that the sender's email address does not match your co-worker's actual address.

Cybercriminals can also register domains that visually resemble legitimate web addresses. In this example, the attacker could register "accounts-amazom.com" and hope the user doesn't notice that Amazon is misspelled.

One of the most common use cases for email spoofing is a scam known as CEO Fraud. This often involves the attacker impersonating someone in upper-level management and emailing other team members requests for wire transfers of money.

Similarly, attackers sometimes impersonate external vendors that organizations use for various services. They might send an urgent email claiming that an attached invoice is overdue. If the recipient opens the attachment, it could infect their device with data-stealing malware (malicious software).

**In all cases, email spoofing is an effective attack method that can yield damaging consequences. So, what can you do to protect yourself and your organization? When handling emails, use this simple, three-step approach:**

- **Slow down**: Most phishing attacks want you to take immediate action without giving it much thought
- **Pay attention**: Attackers love to catch people when they're busy or distracted
- **Inspect thoroughly**: Carefully review every part of an email for potential warning signs

**If you encounter a phishing scam or anything else that seems suspicious, report it immediately.**



SAC the security awareness COMPANY
a KnowBe4 company

# BUSINESS EMAIL COMPROMISE

One of the key indicators of phishing scams is they're typically random, unexpected messages. What if, however, an attacker managed to insert themselves into an ongoing communication thread? That's exactly what happens when someone's email account gets hacked — an attack known as business email compromise (BEC). Let's review an example of how this works.

## Research and Identify the Target

BEC is a bit more sophisticated than the traditional phishing scams you might encounter. In this case, attackers usually thoroughly research the target to ensure they are attacking someone with access to finances. They will also use any information they find to create personalized messages or phone calls designed to gain trust.

## Launch the Attack

With trust established, the attacker will make their move. This involves sending an email containing a malicious link or attachment, either of which can infect the target's device with malware. A successful phish will allow the attacker to gain full access over the target's email account.

## Monitor Communications

Now that the attacker has access, they can sit back and monitor communications between the target and their clients and co-workers. The goal is to identify situations where wire transfers will be involved and when those transfers are expected to occur.

## Hijack the Thread

As soon as it's clear that a payment is ready to process, the attacker will send a message, using the compromised email account, with updated (and fraudulent) payment instructions. Since the message comes from a trusted source in an ongoing communication, the victim usually has no reason to think it's suspicious.

**This type of attack can result in significant financial loss or theft of highly confidential information. That's why it's vital to use caution when handling requests for money or information. Stay vigilant, stay alert, and always follow your organization's policies.**

# ZERO TRUST SECURITY

There was a time when security frameworks used a simple approach: trust but verify. The idea behind this was that a degree of trust is given to people or devices, which are then verified. Entering a username and password to access an account is a form of verification.

That approach made sense because it allowed for efficiency across the security spectrum. But it also means that a cybercriminal will have nearly unlimited access if they successfully hack someone or some system.

Zero Trust changes all of that. It's a model that uses the much more robust stance of "never trust; always verify." This means nothing is inherently trusted at any point, and everything is always verified, often continuously.

Multi-factor authentication (MFA), as a simplified example, is a type of Zero Trust. It requires you to know not just a username and password but also a second code. Meaning, even though you know the proper login credentials, the system still doesn't trust you.



The Zero Trust concept is now used by many organizations. While it's a technical framework that most people don't need to think about, it's also a great concept to apply to your daily security awareness. Here's how:

## Avoid making assumptions.

Attackers want you to assume they are legitimate and trustworthy. That's the whole goal of many scams, especially when it comes to CEO fraud and business email compromise. Never assume someone is who they claim to be.

## Verify before you comply.

If you receive a message from someone you know asking for highly sensitive information, don't simply comply. Reach out to that person directly via a trusted communication channel to verify the request is legitimate.

## Always remain skeptical.

Treat requests for confidential information or money with a high degree of skepticism, regardless of who sent the request. This approach helps prevent attackers from achieving their goals.