SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for Everyone

CEO Fraud/BEC

What Is CEO Fraud/BEC?

Cyber attackers continue to evolve an email attack called CEO Fraud, or Business Email Compromise (BEC). These are targeted email attacks that trick their victim into taking an action they should not take. In most cases, the bad guys are after money. What makes these attacks so dangerous is cyber attackers research their victims before launching their attack. It is also very hard for security technologies to stop these attacks because there is no infected email attachments or malicious links to detect. Here is how the attack works.

The cyber attacker uses the Internet to research their intended victim and people their victim interacts with. For example, if they target you, they would research who your boss is at work or perhaps a real estate agent you are working with from home. The cyber attacker then crafts an email pretending to be one of these people and sends it to you. The email is urgent, requiring you to take an action right away, such as processing an invoice, changing who you make a payment to, or convincing you to reply with sensitive documents. The email works by pressuring you into doing what they want. Here are two examples of how just such an attack could work:

Wire Transfer: A cyber criminal is after money. They research the company you work for, such as identifying who works in accounts payable or anyone responsible for transferring funds. The criminals then craft and send an email to these individuals pretending to be their boss or a senior executive. The email tells them there is an emergency and money needs to be transferred right away to a new bank account. The email pressures them into making a mistake, and in reality, they are sending money to the cyber criminal.

Tax Fraud: Cyber criminals are after people's personal information to use for tax fraud. One of the fastest ways to get this is to steal the information of all the employees at a company. The cyber criminals research and identify who works in Human Resources. They then send fake emails to these individuals, pretending to be a senior executive or someone from legal. The emails create an urgent story, that the tax information on all the employees has to be submitted right away. The people in Human Resources think they are sending the sensitive documents to the senior executive, when they are really sending them to a cyber criminal.

Protecting Yourself

So, what can you do to protect yourself? Common sense is your best defense. Here are the most common clues to look for:

- The email is very short (often only a couple of sentences), urgent, and the signature says the email was sent from a mobile device.
- There's a strong sense of urgency, pressuring you to ignore or bypass your employer's policies. Always follow work-related policies and procedures, even if the email appears to come from your boss or the CEO.
- The email is work related but uses a personal email address, such as @gmail.com or @hotmail.com.
- The email appears to come from a senior leader, coworker, or vendor you know or work with, but the tone of the message does not sound like them.
- Payment instructions are provided, but these instructions differ from ones you already received, such as requesting immediate payment to a different bank account.

If you suspect you have been targeted at work, stop all interaction with the attacker and report it to your supervisor. If you have been targeted at home or you have fallen victim and a wire transfer was made, immediately report it to your bank, then to law enforcement.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Don Cavender *is a former FBI Special Agent, with 22+ years in digital forensics and cybercrime. He most recently targeted cybercrime organizations as the Washington, D.C. BEC Coordinator. He provides training and conducts research in digital forensics and cyber investigations. Find him at* @don_cavender and https://www.linkedin.com/in/donald-cavender

Resources

Social Engineering:	https://www.sans.org/u/HE3
Stop That Phish:	https://www.sans.org/u/HE8
Stop That Malware:	https://www.sans.org/u/HEd
Lock Down Your Login:	https://www.sans.org/u/HEi