Vendor Email Compromise: A Recent Twist in Cybercrime

We Value Your Security | Vol. 2 No. 1

pfm

You receive what you believe is an email from one of your vendors a couple of weeks prior to a deadline for payment of services rendered. This email provides you with new instructions on where and how you should submit the payment.

WHAT DO YOU DO?

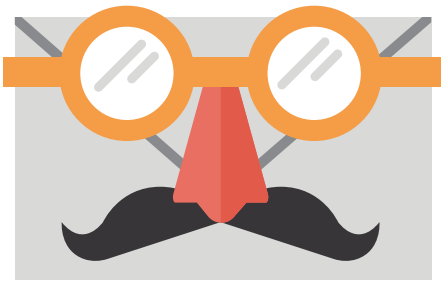
1) Update your records with the new information right away - you really like this vendor and want to demonstrate a good payment history as you want to hire them for more work.
2) Call the contact based on the contact information on the email that was JUST sent to you to verify the update and once verified, ensure your systems are updated.
3) Call a vendor contact based on information you previously received to verify the requested change and if verified, update your systems accordingly.

The use of third-party vendors in your day-to-day operations is often logical and even necessary for banking services, construction or repair contractors, information technology, healthcare, payroll or other services.

While outsourcing these services is necessary, it exposes you to additional risks such as vendor email compromise.

What Is Vendor Email Compromise?

Recently, an attack known as "vendor email compromise" has become more popular and more effective. Vendor email compromise is when criminals use lookalike domains or email spoofing techniques to trick employees into thinking that they're communicating with a trusted contact at a vendor they communicate with on a regular basis. This may prompt employees to reveal sensitive information, submit payment to unauthorized parties, or give unauthorized access to your network.



Emails that appear to come from a trusted source, such as a vendor contact, result in an employee being more likely to consider these emails as legitimate and may respond, click on links, and open attachments, rather than mark the email as spam or junk, or delete the emails.

How Can We Guard Against This Attack?

A large part of cybersecurity is employee awareness and education. This can help protect organizations from vendor email compromise, in addition to phishing attempts, business email compromise and other social engineering attacks. By providing employees with tips to spot or prevent an attack through common-sense methods, your organization can avoid falling prey to an attack.

TIPS TO PREVENT VENDOR EMAIL COMPROMISE ATTACKS INCLUDE:

- Check the domain name to help ensure it was sent from a trusted source. Common tricks for lookalike domains include using a zero (0) instead of the letter "O," using the letters "rn" instead of "m," and using a capital "I" in place of a lower case "l."
- Confirm the email with a trusted contact before taking any action. Call a vendor contact based on information you previously received from the vendor to verify the requested change and if verified, update your systems accordingly. (Correct answer to "**What do you do?**" from above.)
- Use multi-factor authentication whenever possible, especially for sensitive accounts or money movement.
- Focus on looking for anything suspicious or out-of-the-ordinary such as a sudden business protocol change, sense of urgency or typos in the communication.
- Do not click email links. Instead, visit the vendor's website and log into your account from that site. This helps to ensure you are accessing the correct website.

"Focus on looking for anything suspicious or out-of-the-ordinary such as a sudden business protocol change, sense of urgency or typos in the communication."

What Can You Do If You Fall Victim to a Vendor Email Compromise?

If you or an employee fall victim to a vendor email compromise scam, there are a few measures you can take to try to minimize the damage, including:

- Run anti-virus and malware scans.
- Change all passwords and security questions immediately.
- Contact the vendor to inform them of the fraud.
- Notify all financial providers and place stop payments on any payments authorized to the scammers.
- Contact law enforcement to report the incident.
- Conduct post-incident cybersecurity training.

Although nothing is fool-proof, and even the most rigorous cybersecurity program may still be at risk for cybersecurity attacks, promoting employee awareness and education on topics like vendor email compromise attacks can help reduce the risk of a cybersecurity attack.