ORION INVESTIGATIONS

EMAIL BANK TRANSFER FRAUD – AVOID BECOMING A VICTIM

Author – Andrew Smith - Director of Computer Forensics Services

13 January 2022

We have seen a significant increase in the number of cases where employees responsible for issuing payments on behalf of the company have been tricked into transferring the money into bank accounts under the control of a malicious person. **Already in the first 13 days of this year (2022) we have been contacted in relation to three such cases**.

How is this type of fraud achieved and what can you do to prevent your company becoming another victim of fraud via email?

The fraudster will can often gain unauthorized access to an email chain via a number of ways. This includes

- Hacking the company network or your vendor's network
- Unauthorized access by a malicious employee
- Using social engineering or phishing emails
- Using email login details that have become compromised for example by malware located on the computer system or the user using an unsecured WIFI network without a VPN

It should be noted that it is often very difficult to identify how the actual compromise has occurred.

Having gained access to the email chain the fraudster will then create an email address that looks almost identical to an email address within the chain that should be receiving a payment. They will then send an email from the fake email address using an excuse such as ***"our bank account is being audited so you need to make the payment into this other account of ours".*** They will often then follow up with several more emails pushing for the payment to be made as quickly as possible. By using a fake email address, they have now taken control of the conversation. Most victims fail to notice the slight differences between the real email address and the fake one. As a result, all further emails are being diverted away from the intended real recipient to the fraudster. Once the payment has been made it will be extremely difficult to get the money back so prevention is the best policy.

To avoid becoming a victim of the types of frauds described above you should take the following steps:

- Provide cyber-security awareness training for your staff
- Train the staff responsible for making/authorizing payments that if they ever receive an email requesting a payment is made to a new bank account, they should take the following steps:
    - Inform management of the request
    - Examine the email address of the sender carefully to see if it is a fake email address
    - Contact the company direct via telephone and confirm if they were responsible for the request relating to the change of bank account
- When setting up service agreements with new vendors, include a clause in the service agreement detailing the bank account details that payments must be made to and what steps they must take if they ever receive a request to divert money to a different bank account

The above simple steps will help protect your company from becoming a victim of this type of fraud.

If you do find yourself in the unfortunate position of having been a victim of this type of fraud, then Orion may be able to assist in gathering evidence and preparing the evidence so you can report the crime to the police. It is important to take the following steps.

- Retain an electronic copy of all original emails in the email chain and especially the emails requesting payment to a new bank account and any follow up emails from the fraudster.

It is important to keep an electronic copy of the original received emails and not ones that have been forwarded on internally to other staff members. The reason for this is that the emails contain embedded hidden information that is not usually seen when looking at the email through an email client. This information is known as email header information and contains details of all the computers the email has passed through from the sender to the recipient. The email header will also contain time and date information and possibly the originating Internet Protocol (IP) address of the sender. In order for a device to connect to the Internet it has to be allocated an IP address. This IP address will be allocated to the customer by an Internet Service Provider (ISP). Therefore, if we can identify the originating IP address of the email and the time and date information we can identify which ISP is responsible for allocating the IP address and from which country. Law enforcement can then make a legal request to the ISP for details of who the IP address was allocated to at the time and date the email was sent.

When you forward the emails internally the original email header information can be lost which is why it is important to preserve the original emails received in an electronic format.

Case Studies – Examples of cases where we have been able to assist our clients.

Example 1 – A Thai company asked us to examine the emails received from the fraudster to try and identify if they had been compromised or their USA vendor. We were able to show that the fraudster had used the USA vendor email login details to log into the email account via webmail from Nigeria and as a result it was the vendor who had been compromised.

Example 2 – A fraudster had created fake email addresses very similar to our client's legitimate email addresses to commit the fraud. As a result, the other company concluded our client's network had been compromised and they then took our client to court to sue for failing to maintain a secure computer network. Based on the evidence available it was impossible for the other company to draw this conclusion. Orion went to court as the expert witness for our client stating that based on all available evidence at the time it was impossible to conclude how the breach to the email system had occurred and which company had been compromised.

If you need assistance, then please do not hesitate to contact Orion Forensics to see how we may be able to help.