COVID-19: CYBER SECURITY & WIRE TRANSFER RISKS

GRAHAM COMPANY

Preventing Cybercrime and Fraudulent Wire Transfers

COVID-19 has created a "new normal" for how organizations conduct business and how individuals go about their daily routines. The pace of this shift was dramatic, with more than 60% of organizations switching to remote work with very little preparation or analysis of the cyber security impact.

As a result, Cybercrime complaints to the FBI's Internet Crime Complaint Center have increased to over 3,000 complaints received each day. During this pandemic, cybercriminals have become successful through Business Email Compromise scams that result in **wire transfers to unauthorized accounts**. With more individuals working remotely and unable to utilize their standard payment procedures, cybercriminals are applying social engineering techniques to transfer large sums of money and cause financial harm.

Wire Transfer Claim Example: We are aware of loss where a cybercriminal had gained access into the computer system of a company's vendor. The cybercriminal sent an email to this company informing them of a change in wire instructions and to make a payment for services rendered. The company tried to use good cyber risk management and replied that they would call the vendor to verify the new account information. With the cybercriminal already inside their network, the impersonator was able to block this email from going to the intended recipient at the vendor's organization. The cybercriminal impersonated the vendor by calling the company and providing the new account information. By the company not initiating the phone call and dialing the vendor's phone number to verify, they were victim a social engineering scheme and wired a large sum of money. By the time the actual vendor and company realized what had occurred days later, it was too late to recover the transferred funds. It is crucial that the employee who receives the transfer request makes the phone call to the vendor to confirm payment requests and instructions, as we can no longer trust that when we receive a call, the individual on the other end of the line is who they say they are.

Individuals with access to financial information should adhere to the following steps to verify the authenticity of each wire transfer request and prevent wire fraud from occurring:

1. **Pause:** If you receive wiring instructions via a text or e-mail, do not immediately reply. Wait until you have access to a computer to review the request. If you receive a phone call with wiring instructions, inform the caller you must hang up to validate the information.

2. **Instinct:** Utilize your instinct as to whether the request seems legitimate or fraudulent.
   a) Did the individual express urgency or secrecy?
   b) Does the sender's email address, domain name, and signature look right?
   c) Are you aware of any reasons that would result in a change of account numbers?
   d) Did the requestor ask for any sensitive information from you?
   e) Do the instructions or requested amount seem unusual?

3. **Dial:** To confirm you have received a genuine request, use the callback number in the account file. Do NOT use a number listed in the email request or call the number that texted you. There could be a fraudster on the other end of the call. Additionally, it is important that you initiate the call to confirm. Cybercriminals have been successful in not only hacking into the computer systems but the telephone systems, as well, to carry out these scams.

4. **Process:** Only process a payment request after calling a trusted number and receiving verbal confirmation of the transfer request. Verify the wiring instructions and process the payment.

Wire Fraud Prevention Steps

PAUSE INSTINCT DIAL PROCESS

Wire transfers are a lucrative target of fraudulent activity due to the lack of internal controls and employee education, speed of the payment transfer, ease of implementation, and difficulty to recovery and track.

Every organization should have procedures in place regarding the security of their systems and access to funds. Graham Company recommends including the following procedures when receiving an employee banking request change, new corporate wiring payment, or vendor payment request:

1. Utilize multi-level authentication and verification as noted above.
2. Train employees on fraud awareness and reinforce training through simulated phishing attacks.
3. Limit the amount per wire transfer and signoff – for example:
   a) Up to $25,000 can be authorized by one employee
   b) $25,000-$100,000 initiated by Employee A and authorized by Employee B
   c) $100,000+ initiated by Employee A, and cosigned by Employee B and Employee C
4. Maintain a list of all individuals granted authority by vendors to initiate requests.
5. Maintain predetermined call back numbers for frequently utilized vendors or employee banking requests. Never call the number in the email or text or from the phone request.
6. Create challenge questions or a PIN # for access or changes to wiring instructions that must be answered via phone and would not be known through an internet search.

Ensure employees handling payment requests know that each step is vital. They are not being a hassle to others by taking the precautions and each action is pertinent in identifying fraudulent requests which could be detrimental to the organization.

In addition to sophisticated procedures being implemented, insurance can be a supplemental line of defense to protect an organization's assets. Organizations cannot ignore the challenges and emerging risks associated with remote workforces and should work with their Graham Service Team to maximize the value of their cyber insurance policy, understand how their policy would respond to a cyber incident, and discuss risks and exposure. Graham Company is equipped with cyber insurance expertise to educate IT, management, legal, and senior executive stakeholders.

Please reach out to a member of your Graham Service Team to have further discussions.