Wire Transfer Fraud on the Rise â€“ A Warning for Businesses and Consumers Alike

April 14, 2015 â€“ Over the past few years, the use of wire transfers to move funds has grown exponentially. Whether to pay for credit card bills, purchase real estate or used in the day to day operations of businesses, wire transfers have become easy to use. And for businesses, they are often less expensive that writing a check. But the growth in wire transfers has also attracted the attention of criminals. Thatâ€™s a trend that we donâ€™t think will change any time soon, and which could prove to be very expensive for victims.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The hackers behind wire transfer fraud are operating without a lot of resistance. And they donâ€™t even have to be very sophisticated hackers in order to be successful.

Typically, they will target a person or company that they have reason to believe is using wire transfers. They will attempt to plant a virus or Trojan horse on the victimâ€™s computer. That virus will then monitor all of the email being sent out and received through the infected computer. All the hacker has to do is sit back and wait until an email with wire transfer instructions is sent by the victim.

As soon as that happens, the hacker will spoof the victimâ€™s email address and send out a follow-up message. This second message can contain a variety of information but will likely say something like, â€œI just realized that I sent you incorrect wire transfer instructions. Please wire the money toâ€¦â€• At this point, the hacker will provide another bank account and routing number which is likely off shore.

Once the follow-up message is received, there is a very good chance that the recipient will follow the instructions. There

are a variety of reasons for this. In the case of businesses, many of them do regular wire transfers. The person receiving the follow up message could work for the businesses bank or be a supplier. Either way, if the transfer isnâ€™t out of the ordinary and if it looks like it came from the correct email address, the recipient may very well not question the instructions.

Consumers can also get caught up in this scam. This is especially true in real estate transactions when buyers transfer large sums of money for their initial deposits and down payments. The targets for hacking in this case include real estate agencies, escrow companies and known investors.

As inconvenient as this sounds for consumersâ€¦ who do have protection against bank fraudâ€¦ it can be much worse for businesses. Thatâ€™s because businesses are expected to implement reasonable security measures to prevent hacking and fraud. If money gets incorrectly wired out of your business account because you didnâ€™t scan your computer for viruses, there is a very good chance that your business will never be reimbursed.

Consumers are protected for charges in excess of $50 if the crime is reported right away, but even this could prove to be problematic. Thatâ€™s especially true in the case of real estate transactions which are often timed to be coordinated with other like transactions. If the money disappears and the buyer canâ€™t replace it with other funds, there could be a variety of legal and financial implications.

Any business that uses wire transfers should implement security procedures to govern those transfers. Computers should be checked regularly for viruses and updated with the most current security patches. If the computers are installed on an office network, then every computer on that network needs to follow the same security procedures.

In addition, businesses should insure that they are with appropriate people at their bank or with their vendors, prior to sending a wire transfer out. And they should have a procedure in place which states that any changes to wiring instructions require a phone call rather than an email. Their banks and vendors need to be aware of this policy and need to know that if they donâ€™t follow it, they will be held accountable. This may be difficult to implement for small businesses, but larger firms should have the ability to force their partners to comply.

Consumers who are doing wire transfers probably shouldnâ€™t send wire transfer instructions via email. Instead, take a moment and pick up the phone and provide your information that way. It may be a little less convenient but it could save you many sleepless nights.

Anyone who believes that they have been victimized in the way described above should contact their local FBI office and ask to speak with someone in their cybercrimes unit.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS