Protecting Yourself

From Real Estate Cyber-fraud

Sensitive information plays a critical role in your real estate transactions, and it's imperative that this information remains safe and protected. When you order policies from Stewart Title you can do so knowing that confidential and personal information is protected through our robust data security methods. But, as a legal professional, there are steps you can take to protect yourself from cyber-fraud too.

Recently, there has been a wave of cyber-fraud. Cybercriminals hack into the email accounts of legal professionals or other persons involved in real estate transactions. These "hackers" are patient; they sit and wait until they discover useful information to assist in the scam and trick you into sending money through a wire transfer to a bank account that appears to be legitimately owned by a party involved in the transaction (but is not). The hackers send an email that appears to be from an individual involved in the transaction (a practice called spoofing).

At first glance, these spoofing email addresses appear legitimate but often have one additional letter or some other minor variation from the actual email address.

Example: msmith@stewartttitle.com
instead of
msmith@stewarttitle.com

These spoofing emails advise the recipient that there has been a last-minute change to the wiring or payment instructions and request that funds be sent to the new account information provided. By following these instructions, the funds are inadvertently wired to the hacker's account and, most often, lost forever.

Other types of cyber-fraud

Ransomware

This type of attack involves the theft of data or locking the company out of their data systems. The criminal then demands payment of a "ransom" (often in bitcoin) to release your data.

These attacks generally occur when someone unwittingly opens an email, attachment, or by clicking links on unsecured websites. Ransomware can also originate from third-party vendors who are unaware they are infected.

Example:

In 2017, a global law firm suffered a ransomware attack that effectively paralyzed the firm. This attack required over 15,000 hours of IT overtime to recover their computer systems and impacted their ability to service clients while the attack was occurring.

Phishing Scams

These scams originate from bogus emails or website pop-ups that contain links to entice the receiver to inadvertently download malware.

Example:

A clerk received an email with an invoice attached. The invoice turn out to be fake and led to the downloading of spyware onto the network. Criminals were then able to monitor the clerk's computer activity and obtain bank account information, passwords and wire transfer information. Without the clerk's knowledge, funds were then wired from the lawyer's/notary's trust account overseas.

Read More

stewart TITLE

Recognize common indicators of cyber-fraud

- Emails requesting last-minute changes to wiring information (e.g., particularly changes in the beneficiary and/or receiving bank)
- Requests for wire transfers late in the day or week or outside of business hours
- Emails with poor grammar and/or typographical errors
- Slight, typically unnoticeable-at-first-glance changes in the email address

Suggested best practices for transmitting and receiving sensitive information

- Send emails with sensitive, personal information, through encrypted email only
- Verify requests to change wiring instructions through a trusted method (like a phone number previously verified); never use the phone number in the email
- Verify wire transfer requests to locations outside normal business areas
- Never click on any links in an unverified or unexpected email
- Always question attachments and links that are sent unencrypted

Additional tips to minimize cyber risks

- Conduct annual training on cyber security for all staff
- Do not open emails you do not recognize until they are verified
- Do not follow unusual instructions about banking information or funds transfers, etc. without verifying
- Never use email addresses or phone numbers within suspect communications to verify
- Look for spelling and grammar errors in emails (i.e., company names or standard terms)
- Hover your cursor over the hyperlinks without clicking to see actual URL of the link. If the address is different than what is displayed, it's likely a phishing scam
- Have proper IT support for computer systems
- Ensure virus detection software is up to date
- Use encryption for sensitive data
- Have password strength policies and enforce them
- Maintain proper back-ups of your electronic data
- Have a plan in the event you suffer a breach and know who to contact and how to recover data from back-ups effectively
- Consider insurance for cyber breach losses

What to do if you believe you are a victim of cyber-fraud

- If money was wired in response to fraudulent wiring instructions, immediately call all banks and financial institutions that could put a stop to the wire or your funds
- Contact your local police or local municipalities' real estate fraud division
- Contact any other parties who may have been exposed to the cyber-fraud so that appropriate action may be taken
- Change all usernames and passwords associated with any account that you believe may have been compromised
- Report any cybercrime activity to the RCMP National Cybercrime Coordination Unit https://www.rcmp-grc.gc.ca/en/nc3

Contact us for more information.
888.667.5151
stewart.ca

stewart™ TITLE