PENNSYLVANIA LAND TITLE ASSOCIATION

ORGANIZED 1921

CyberSecurity Tips - You Need To Know

Consumers, title agents and real estate agents are frequently the targets of phishing emails, which are used to gain access to their technology infrastructure. **Be careful what you click on!**

Important safeguards include:

- Install software and antivirus updates; they contain security patches that will keep your system protected.
- Never use “free” email accounts. Always use encrypted email accounts with end-to-end encryption.
- Keep files containing Non-public Personal Information (NPI) off all mobile devices and computers.
- Use strong passwords and change them every 90 days. Use passwords that include a combination of letters, numbers and symbols and have a minimum of 12 characters OR use a word passphrase for added security.
- Do NOT use the same password for multiple logins.

- Consumers should verify settlement information (i.e.: wire instructions) directly with their title agency.
- Make sure all parties understand the transaction process at the beginning of client engagement.
- Wire instructions are unlikely to change. Detailed wire instructions will be provided when the order is initiated.
- Verify any requests to change wire instructions with the customer in person or via phone using contact information that is already on file.
- Be aware of Display Name Spoofing in emails, which impersonate a trusted individual or company in an attempt to get your personal information. These email addresses are modified to impersonate someone you know.
- Do NOT use the phone numbers in an email, especially if it contains wire transfer information.
- Always require and confirm dual or multifactor authentication on all financial transactions and transfers.

- Confirm the name on the account **before** sending wires and verify receipt within four hours of the transfer with your real estate professional or title agent. Detecting fraud within 24 hours gives the best chance of recovery.
- Realtors and Title Agencies should have proper insurance: cyber liability, E&O, and crime policies.
- Virtual Private Networks (VPNs) sound complicated, but are very easy to use and definitely safer than public networks! Any remote access should be through a VPN. Simply put a VPN is a service that allows you to access your server or the web safely and privately by routing your connection through a secure server and hiding your online actions.
- Immediately notify your financial institution and request a recall notice of a wire transfer if you have been victimized. Then you should ask the financial institution that received the funds to freeze the account due to fraud.
- If you are a victim of wire fraud, contact your local FBI office and police to report the incident.
- Report any and all incidents to **IC3.gov**, the FBI’s Internet Crime Complaint Center, even if there have not been monetary losses.

This publication is designed solely to assist real estate professionals and consumers as educational material in protecting against cybercrime. This is for informational purposes only and should not be considered legal advice. For specific assistance please contact your IT professional or legal counsel.