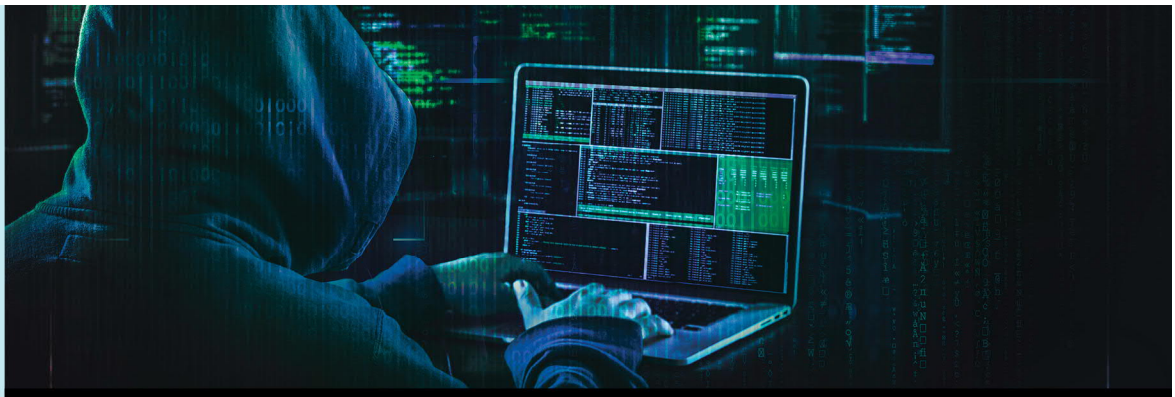
SHINE BRIGHT



WORKING TOGETHER TO PREVENT WIRE FRAUD

Telephone and email scams targeting real estate and title/settlement are rising sharply, according to reports from the FBI and the Federal Trade Commission, which reveal an 1,100 percent rise in business email compromise (BEC) last year and more than 250,000 spoofed phone calls alone.

Cybercrime has become so common, that the FBI has created an Internet Crime Complaint Center (IC3) to address them.

Most commonly, as Forbes Magazine notes, a scammer will hack into a buyer's email and monitor it. When the scammer sees emails between the buyer and the real estate agent, they wait until the transaction is imminent and at the last minute, they send the buyer a fake email made to look like it's coming from the agent and asking the buyer to wire the purchase money to a different account - which, of course belongs to the scammer.

Many such scams occur on Friday afternoons, the FBI says, especially the Friday before a long weekend. By the time victims realize they have been scammed, three or four days have gone by, and the chances of getting their money back are almost nil.

In the title industry, scams originating from SpoofCard calls can be a nightmare, according the American Land Title Association (ALTA.) The technology provides criminals the ability to change what someone sees on their ID display when they get a phone call, so they think the call is coming from one person when it's actually coming from the scammer.

Real estate experts have been working diligently to tighten telephone and email security. Many are using identity protection services specifically designed to help protect consumers from fraud, and redoubling efforts to provide ongoing training to employees and customers alike.

As your title partner, we take seriously the obligation to protect real estate professionals and their clients. We mandate ongoing and in-depth education and training updates to our employees, and provide strict wire fraud warnings with every communication we send. We clearly and consistently caution consumers to call us at a number they know is accurate before wiring any funds, and warn them never to use a potentially spoofed phone number they received in a last-minute phone call or email.

- We can take these specific actions to protect against escalating BEC disasters:
- Implement good password policies and back them up
- Use dual-factor authentication for password updates
- Use firewalls, anti-malware, software., phishing detection, and a secure internet gateway
- Employ the services of a company that monitors the dark web and alerts you if employee identity or credentials are stolen

By arming ourselves with the proper knowledge and business tools, and ensuring that our clients are kept aware and vigilant, we can rest a little easier and guard against the ever-evolving schemes of wily cybercriminals.