FBI and NAR offer 10 ways to guard against real estate cyber scams

Although technology has made real estate transactions quicker, more seamless and increasingly transparent, it has also made buyers, sellers and real estate professionals vulnerable to cybercriminals looking to cash in. In the past year, $969 million have been stolen from buyers via escrow scams — something cybercrime professionals say will continue to grow in popularity.

Last week, 100-percent commission real estate franchisor Realty Executives hosted a webinar to educate agents and brokers about wire fraud, and National Association of Realtors (NAR) senior counsel Finley Maxson and FBI supervisory special agent Martin Hellmer both attended. They said awareness, education and preparedness are key in safeguarding your business and your clients.

Hellmer said businesses usually focus on having top-notch technology and cybersecurity, but forget to educate employees on best practices, which he called a major mistake.

“We typically think of these magnificent young minds at the command line and typing things we don’t understand — and a lot of hackers are that good — however, the primary entryway into the front door is through phishing emails,” Hellmer said in the webinar.

“We as humans are curious, and we are usually the ones who give the bad guys access. Our computer networks and systems may have the best protection in the world, but it doesn’t mean a thing if an employee or you click on that phishing email.”

Here are their tips for combating cyber scams:

Real estate sales Jedi mind tricks

Plant the seeds of action in prospects' minds READ MORE

1. **Update the software on your phone, computer, tablet and any other electronic device regularly.** It's often annoying to download and install regular updates of your operating system, but you wait to update your device's software, Maxson and Hellmer say you're giving criminals the opportunity to take advantage of any security weaknesses.
2. Air-gap **computers that have sensitive information.** Air gapping is when you make sure the computer isn't connected to the internet or to any other computers that themselves are connected to the internet. It's much more difficult to remotely hack an air-gapped computer.
3. **Regularly back up all your electronic devices.** If you're hit with ransomware–malicious programs that hackers use to lock your computer and hold it hostage in exchange for money, usually a digital currency–you can restore your computer to the latest backup. Maxon and Hellmer also suggest never paying the ransom to get your information back, even if your computer isn't backed up.
4. **Make sure no one can access all of your business information.** The sales team should

only have access to information pertinent to their team. This prevents hackers from being able to access the entire network through one person.

5. **Strengthen your passwords.** Use passwords that are 10 characters or more, and take advantage of two-factor authentication to protect your emails.
6. **Be aware of common email scams.** For example, escrow scams where criminals pose as a title company and change the wiring instructions, referral scams where criminals promise to send a lead for a small fee, and fake Docusign emails and texts with links. These are all ways criminals can gain access to your information.
7. **Implement state-compliant policies.** This includes policies for handling and disposing personally identifiable information (PII), such as social security numbers and bank information. Also create policies for document protection and disposal, breach notifications and cybersecurity. These measures help reduce the risk of being hacked, and they help if you're ever civilly sued for negligence.
8. **Conduct voluntary security audits.** Hire a security expert who can identify weak points in your systems and offer solutions for strengthening them.
9. **Invest in cyber insurance.** This will cover the costs of restoring the network and the data, providing breach notifications and credit monitoring.
10. **Make sure your vendors are following proper cybersecurity protocols.** Closely read over the security and privacy policies of the companies you work with and rely upon, and find out what recourse you have–if any–if they are hacked and your information is exposed.

Email Marian McPherson.

Source: click here