WIRE FRAUD SMISHING RANSOMWARE

COULD YOU BE THE NEXT VICTIM OF A CYBERCRIME?

Use these tips to avoid falling for common internet, email and phone scams.

BY TOM GIL

Here's a hypothetical for you. You click on the wrong link and suddenly you're locked out of all the information on your computer—client data, photographs, financial information, you name it. You receive a message that says you must pay to unlock your information. If you don't, it will be destroyed. That's ransomware, a type of malware that locks up a person's computer and threatens to destroy all files until a ransom is paid. **Only, it's not a hypothetical.** It's happening to real estate agents and brokers around the country. One Florida real estate professional was able to reset their computer and restore from a backup, but many aren't so lucky.

A hot housing market and loads of sales yield lots of money transactions, and that means criminals have more targets on which to prey—agents, brokerages, buyers and sellers. According to the FBI's Internet Crime Complaint Center, there were more than 11,000 victims of real estate cybercrime in 2019. And says cybersecurity firm PurpleSec, cybercriminals are taking advantage of the pandemic to send sophisticated phishing email schemes, where an email seems to come from a reputable company to get recipients to reveal personal information, such as bank accounts or passwords.

Cybercriminals don't differentiate between real estate sectors. They attack all players in the space equally, including agents, buyers, escrow firms, insurance agents, inspectors and even title companies. The 2019 hack of the First American insurance company exposed the data of almost 900 million customers. This led the National Association of Realtors® to ensure that any future privacy law consider smaller businesses and individual Realtor® agents when drafting them.

WHO'S IMPACTED?

It's important to understand that cybercrime can affect real estate agents in many ways. "It doesn't have to be something directly related to their business," says John Iannarelli, a retired FBI special agent and expert on cyber and counterintelligence investigations. "It could be attached to a message sent to your cell phone, where you get a text message with a link that downloads malware to your phone. That's called smishing.

However, Iannarelli says that the biggest cyber threat to real estate professionals is business email compromise. "In the world of property sales, when it comes time to make a payment, these hackers will get into real estate agent and title company email accounts. When it comes time to wire the money, they jump in, create an email address to appear as if they are the trusted Realtor®, and send false wire instructions. Next thing you know, the money is gone overseas never to be seen again," he says.

The losses can be significant. "Last year, we documented $3.5 billion in losses," says Iannarelli. "Those are just the people who took the time to file a complaint to the FBI."

HOW TO PROTECT YOURSELF

But you can protect yourself, other than avoiding clicking on links and filling out personal information online. Here are some tips:

1. Train people on cybersecurity. "Brokers and managers: Don't assume everyone on your staff knows what they're doing," says Iannarelli. Teach your agents and staff about the red flags.

5M3PHOTOS/GETTYIMAGES.COM

CYBERSECURITY CHECKLIST: Best Practices for Real Estate Professionals

Cybercrime can be devastating to real estate professionals and their clients. The following checklist offers some best practices to help you curb the risk of cybercrime. Because data protection and cybersecurity laws differ across the country, NAR® recommends that you work with an attorney licensed in your state to help you develop cybersecurity-related programs, policies and materials.

Email and Password Hygiene

- Never click on unknown attachments or links, as doing so can download malware onto your device.
- Use encrypted email, a transaction management platform or a document-sharing program to share sensitive information.
- Carefully guard login and access credentials to email and other services used in the transaction.
- Regularly purge your email account and archive important emails in a secure location.
- Use long, complicated passwords such as phrases or a combination of letters, numbers, symbols.
- Do not use the same password for multiple accounts.
- Consider using a password manager.
- Use two-factor authentication whenever it is available.
- Avoid doing business over public, unsecured Wi-Fi.

Other IT-based Security Measures

- Keep antivirus software and firewalls active and up to date.
- Keep your operating system and programs patched and up to date.
- Regularly back up critical data, applications and systems, and keep backed-up data separate from online systems.
- Don't download apps without verifying that they are legitimate and won't install malware or breach privacy.
- Don't click on links in texts from unknown senders.
- Prior to engaging any outside IT provider, review the applicable privacy policies and contracts with your attorney.

Law, Policy and Insurance Considerations

- In collaboration with your attorney, develop a written disclosure that warns customers of the possibility of transaction-related cybercrime. Florida Realtors® has created a Wire Fraud Email Notice (WFPN-3) that you and your counsel may use and adapt.
- Stay informed on Florida's laws regarding personally identifiable information, the development and maintenance of cyber and data-related business policies, and other required security-related business practices.
- Develop and implement the following policies:
  - Document Retention and Destruction Policy
  - Cyber and Data Security Policy
  - Breach Response and Breach Notification Policy
- Ensure that your staff and licensees have reviewed and are following all implemented policies.
- Review your current insurance coverage and ask your insurance agent about cyber insurance and the availability and applicability of products such as social engineering fraud endorsements and computer and electronic crime riders.

Source: National Association of Realtors®

FLORIDA REALTORS® TAKE 5 VIDEO

Wire Fraud Is on the Rise—Here's How to Protect Your Clients

Buyers are being bilked out of hundreds of thousands of dollars by criminals using sophisticated software to hack email accounts and looking for keywords that indicate a transaction is in progress. Here's what you need to know and what Florida Realtors® is doing to keep you on the right side of the law: **floridarealtors.org/wire-fraud**

Require them to change passwords frequently and talk about the different scams out there.

2. Require confirmation of wiring instructions. "Tell your customers that they need phone confirmation before they wire any money. It's not enough for the real estate agent to verify they received your email, because they may have sent an email that the hacker intercepts and deletes before they send a fraudulent one," he notes.

3. Know your Information Technology (IT) people. Did you do a background check on your IT person? "Many IT people got into the profession because they were hackers and decided they needed another way to make a living," says Iannarelli. "I've arrested many of those over my FBI career." He suggests you use a reputable, established company and make sure you properly vet any new hires.

4. Back up everything, daily or hourly. "Aside from good cybersecurity basic protocols, you must have everything backed up. We have to wipe the hard drives to make sure hackers can't come back in again, but that means you'll lose all of your data unless you have a backup," he says. The backup needs to be separate from the main services, such as an external hard drive or in the cloud.

5. Know your FBI office. Know the point of contact to call in case you've been a victim of a hacker or cybercrime. But, more importantly, says Iannarelli, "The time to contact the FBI is not when you're a victim. Build that relationship. There are also public-private alliances that you can join, such as InfraGard," he says. "They will send you frequent notices about the types of threats out there.

6. Use a Virtual Private Network or VPN. "I'm a big fan of encrypting any sensitive financial information, which is easier than people think," says Iannarelli. "VPNs are inexpensive and anything private sent through one can't be seen by a hacker. Although, it won't help you with a ransomware attack. Avoid any free Wi-FI networks, such as the one at your local Starbucks.

According to Iannarelli, "If you make yourself just a little more difficult to hack into, they're going to go after the easier targets. They're not going to waste the time. So, by just taking a few simple steps, like using an encryption service, and picking up the phone to confirm wire info emails before initiating the wire, it will make you a harder prey and a less likely target."

He adds, "Hackers don't have to hack 100 different places, they need one transaction with one real estate agency, and can steal six-seven figures easily. But the business loses their brand reputation and customer confidence, which is much harder to recover."

By taking small incremental steps inside the organization to improve awareness using periodic training sessions, and by teaming your lawyer with a vetted cybersecurity service provider, you can avoid a brand-tainting catastrophe, and sleep easier at night knowing that you learned how to outrun a bear in the digital forest of cybercrime. #

Tom Gil is U.S.-based freelance writer.

Common Real Estate Scams

Florida Attorney General Ashley Moody issued a warning for Floridians to remain vigilant against real estate scams. Common real estate scams include escrow wire fraud, rental scams, loan-flipping scams and foreclosure relief scams. While they aren't all cybercrimes, it pays to know about all types of scams.

ESCROW WIRE FRAUD

In escrow wire fraud, scammers usually pose as representatives from a title or escrow company and contact a new homebuyer with instructions for escrow money transfer. If the consumer follows the scammer's instructions and wires in the escrow money, the scammers can withdraw that money and disappear.

To avoid this trap, consumers should always check the original documents received from the lender directly rather than relying on just an email, and they should call the phone numbers listed on the original document to confirm the validity of the wiring instructions. A big red flag: Sometimes an email requests an escrow change that contradicts instructions already received. Always confirm an escrow account number with the bank or lender before wiring money.

RENTAL SCAMS

Scammers post fake rental ads on websites, often using real photos and/or addresses taken from a legitimate real estate listing or rental offer. They change only the contact information.

Once a consumer expresses interest in the rental, the scammers ask for either an upfront cash payment to rent the property or money for a deposit. Consumers should be suspicious of anyone who asks for a cash deposit to see a property, and ensure the person is the real property owner before negotiating rental terms. A big red flag: Scammers will often say they're out of town and suggest that renters drive by to look at the property. They often "scrape" information from an actual listing because the home will then have a "for rent" or "for sale" sign in the yard.

LOAN-FLIPPING SCAMS

Loan-flipping scams occur when a predatory lender persuades a homeowner to refinance their mortgage repeatedly, often borrowing more money each time. The fraudster charges high fees with each transaction, and eventually the homeowner gets stuck with higher loan payments they can't afford.

FORECLOSURE RELIEF SCAMS

In a foreclosure relief scam, criminals dupe homeowners in pre-foreclosure with a promise to save the owner's home–providing the owner pays a large upfront fee. As time passes, these homeowners often find themselves in worse financial shape and living in a house that the bank has still foreclosed. Consumers should work directly with their loan servicer to modify an existing loan, request forbearance or make another arrangement.

Real estate scams in Florida can be reported to the Attorney General's office by calling (866) 9NO-SCAM or filing a complaint at MyFloridaLegal.com.