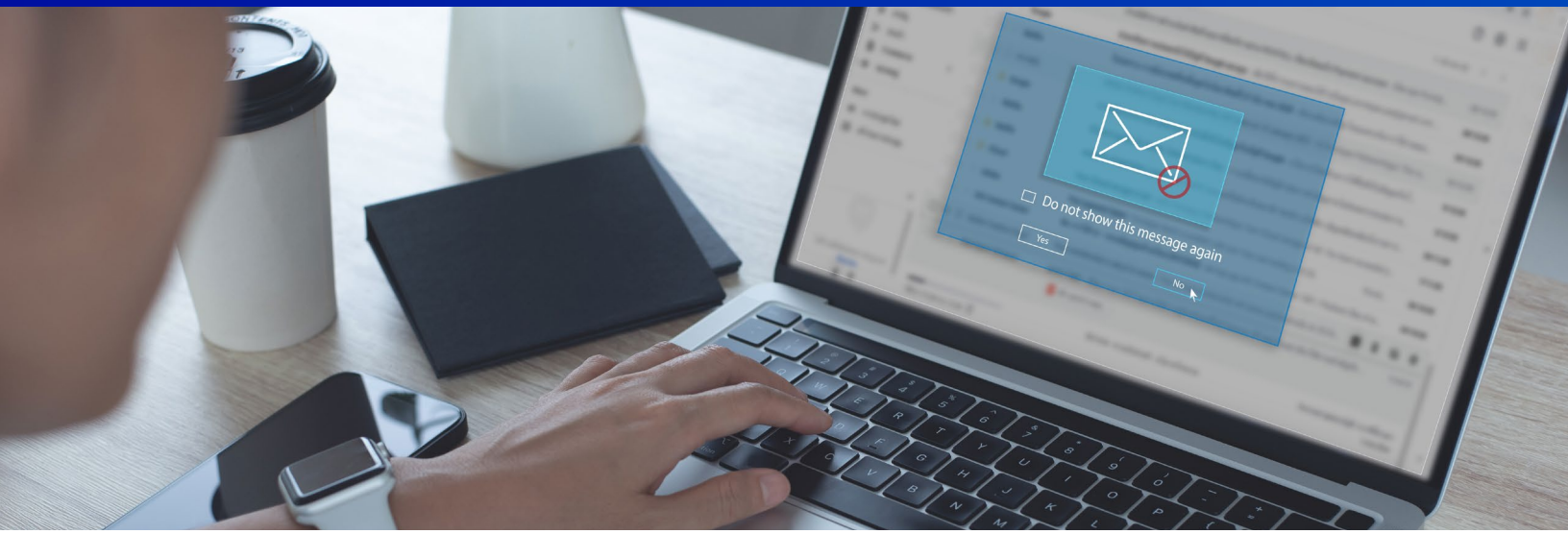
Vol. 7 / Issue 4

doma

# NewsLink

## Investing in Secure Email: The First Line of Defense Against Cybercrime




> Cybercrime is on the rise, according to the FBI's Internet Crime Complaint Center (IC3), and unfortunately, your real estate transaction may be in the crosshairs.

According to a report issued by IC3, cybercrime complaints rose to nearly 850,000 in 2021, a 7-percent increase from 2020. Potential losses exceeded $6.9 billion, with business email compromise/email account compromise (BEC/EAC) schemes accounting for nearly $2.4 billion. Many of those losses were experienced by homebuyers, sellers, escrow companies, and lenders, as cybercriminals have discovered easy targets in the unprotected emails of the participants in the real estate transaction.

While losses continue to snowball, there are steps real estate agents can take to protect their homebuyer and seller transactions. To assist you in those efforts, we offer this overview of BEC/EAC schemes as well as effective prevention tactics.

### Cybercrime Schemes

BEC/EAC is a cybercrime scam targeting the communications between businesses and individuals involved in financial deals, such as real estate transactions. Fraudsters use social engineering to infiltrate the transaction, often pretending to be one of the parties to the transaction, to direct funds to fraudulent accounts. Here are some of the tactics cybercriminals use to reel in their victims:

#### Phishing

Phishing emails are sent to victims to gather data by asking the recipient to provide information or click on a link. The email may include a special offer or invoke a sense of urgency about an imminent account closing.

It may include attachments to be downloaded for more information, which can contain malware that can harm your computer.

## Spear Phishing

Spear phishing is more targeted, usually coming from an email faked to look like someone the recipient knows, for instance a coworker, a vendor, or a customer. Once again, the fraudster is encouraging you to click on a link that may contain malware or asking you to provide confidential information.

## Spoofing

Spoofing is simply masquerading as someone else. It is the tools and subterfuges criminals employ to get you to believe the email is from a legitimate source. For instance, the fraudster may create email addresses that are one letter off from a known customer or coworker. They may insert purloined logos to create an official looking email.

## Smishing

Smishing is when you receive a text message that urges you to click on a link or send information, once again creating a sense of dread or panic so that you act quickly without thinking through the request or any negative ramifications.

## Vishing

With vishing, an employee receives an email invitation to attend a video conference, purportedly from a manager. In the conference, the fraudster shields their identity by claiming their video is not working properly and then instructs the employee to initiate a wire transfer to a fraudulent account.

Although it is important to be able to recognize the tactics cybercriminals use to gather information, it's even more important to stop the intrusion to begin with. Here are some defenses you can employ to minimize the likelihood of the cybercriminals getting a foothold in your system.


## Secure Your Computer

Your company may have an IT department providing all the necessary system protections that you need. But if you are on your own, make sure you have robust anti-virus and anti-malware solutions protecting your computer. Here are some solutions on the market:

- Bitdefender
- F-Secure
- Intego
- Kaspersky
- Malwarebytes
- McAfee
- Norton

If you are unsure which one is best for you, check out **7 Best Antiviruses for Small & Large Businesses in 2022** on safetydetective.com, which provides helpful details on each of the solutions.

## Secure Your Email Accounts

In this era of increasing BEC/EAC fraud, it's imperative that real estate agents take steps to secure their email for the protection of their homebuyer and seller customers.

If you are currently using Gmail or Yahoo for your email communications, remember that these emails are free because Gmail and Yahoo can scan your communications. They do this to gather information for marketing purposes. With these types of systems, you aren't getting the highest level of security that your real estate transactions require.

There is no more vital commitment you can make this year than to move your email communications to a secure platform to protect you, your clients and your transactions. **Here** is a list of the top 10 services that provide enhanced email security for small businesses: cybernews.com/secure-email-providers/

## Secure Your Clients

Now that you have secured your systems and your email, it's time to secure your clients.

Acknowledging that most of your customers are not operating on secure servers or communicating through encrypted emails, the best way to help them stay secure is through education. Here are some tips to share:

### Social Media Silence

Warn your clients to refrain from posting anything about their proposed home purchase or sale on social media until the transaction is complete. Posting information invites cybercriminals to access details they can use to infiltrate the transaction.

### Personally Identifiable Information

Educate your clients on what is considered personally identifiable information (PII) and advise them never to email this information, no matter who requests it. PII should only be shared in person or through protected portals.

### Identity Theft

Provide them with information about the risk of identity theft and how they can protect themselves.

### Cybercrime

Explain the dangers of social engineering, phishing, spoofing and other cybercrime tactics, providing specific examples of emails, texts, or phone calls for which they should be on the alert.

Advise them to avoid responding to any suspicious communications and to report them back to you or to the title company.

### Malware

Remind them never to click on unknown links in their email to avoid possible malware intrusions into their computer.

### Wiring Instructions

Advise them that their lender, title agent, escrow officer, or closing agent will never make changes to wiring instructions via email. If there is any need to change wiring instructions, it should always be done in person and/or verified using a trusted phone number.

### Safety Zone

Provide them with phone numbers they can safely call to verify any requests for information.

### Stop, Look, Listen

Advise them to slow down if an urgent demand is sent their way and to be proactive in following up in person or by phone with you or the title company on any odd requests to verify information they have already provided.

Magnolia TITLE COMPANY, LLC

A Publication of Doma Title Insurance, Inc.