
HARDENED
Del
delete
F12
F11
F10
F9
F8
F7
enter
return
shift
End
PgUp
PgDn
Home
alt
option
command

Brian Bosscher
President and founder
Condo Control

Cybercrime

Protecting your Corporation's Digital Assets from Threats and Thieves

Have you ever received an email where your boss or colleague asks you for a weird favour? One of the most common odd messages is a request for iTunes gift cards, but other variations either ask you to make a purchase with your own money and send PINs to the requestor or share your personal information.

Most of us are aware that these types of emails are not from anyone we know. These 'phishing' or scam emails are distributed by hackers impersonating people in our contact lists, hoping that we don't notice the incorrect sender address or numerous typos. Nevertheless, these fake emails can catch us off guard when we're in the middle of a busy workday, and they have the potential to compromise our personal or confidential information.

Unfortunately, as a company that works with hundreds of condo buildings, we've heard about many email hacking incidents. Secure platforms like Google or Outlook filter out some obvious scam emails, but the senders get more clever and learn to get past those filters.

Property managers get tons of emails each day and may or may not see the warning signs that they've opened a malicious message. If they click on a link or send some sensitive information, they could expose the entire corporation. Hackers will take the sender's money or data, but some skilled thieves may use ransomware to gain administrative access to the property manager's computer. It's a rare but very real possibility.

These are some of the main ways hackers will get a hold of a property manager's email address:

- ***Buying email lists***

Hackers know where to look to buy email lists. Some lists have thousands of email addresses. Fortunately, most people who buy lists to send spam emails get caught. That's because email service providers are serious about their users sending permission-based emails. Any campaign that gets flagged as spam may result in the sender getting kicked off of the platform.

- ***Harvesting emails***

Spammers can also harvest emails. They instruct a bot to crawl the internet and find the "@" symbol in this instance. Emails are then added to a list. Property managers can avoid this by spelling out

their email (using [at] instead of @) so the bots can't detect it.

• ***Data breaches***

Through stealing data from one victim, hackers may get a hold of many other email addresses, credit card numbers, login credentials, etc.

Ransomware is a form of malware that encrypts files. Ransomware infects a computer when a file, which looks harmless, is opened by the victim. More aggressive forms of ransomware exploit security weaknesses to infect computers without needing to trick the recipient. Once the ransomware is active, the hacker will demand a ransom, usually money, from the victim in exchange for restored access to their data.

Ransomware can be expensive and result in significant data loss. A property manager could end up losing passwords, financial data, records, or worse, personal information belonging to the condo owners.

While it is hard to prevent all spam emails from getting through to your inbox, there are steps property managers can take to prevent sensitive information from ending up in the wrong hands.

• ***Two-factor authentication***

While it's a simple and highly effective way to keep all accounts safer, two-factor authentication (2FA) remains an underused security measure. Virtually every email account, software system and social media app have a 2FA option. But because it can be a modest inconvenience, many people opt not to use it.

We strongly encourage property managers, and everyone for that matter, to use this safeguard because it makes it harder for attackers to gain access to any account. Knowing the password is not enough to gain entry. The person trying to log in must also provide a unique code sent to or obtained through the rightful account owner's phone. Without both pieces of information, a hacker cannot access valuable digital assets stored on password-protected email accounts or software platforms.

• ***Configure permissions for minimum access***

Property managers are advised to give colleagues, board members, contractors, etc., the minimum access required to do their job, but never more. If team members need more access later, it's not hard to grant authorization at that time. Operate on a need-to-know basis. Don't volunteer access if someone doesn't need a login to an account or permission to use specific folders. This allows PMs to control sensitive information better and limit exposure. The fewer people that have access to sensitive data, the less likely it is to get hacked.

• ***Learn how to identify high-risk emails***

We understand how busy property managers are, but taking 20 extra seconds to examine emails for red flags can help keep their condo's data a lot safer. There are always some telltale signs that a hacker has sent a message.

The first thing you should do is check the sender's email address. Often, it will consist of a bunch of random letters and numbers, like ontariogov123abc@fakemail.com.

The second thing to consider is if this message is well-crafted or carelessly thrown together. Does it have several spelling errors? Are there capitals where there shouldn't be? Does the signature look correct? A careless email could be a sign that it is fake.

Thirdly, if the sender claims to be someone you know, does the tone match how they usually write emails? Has your colleague ever asked you to buy something for them before? Would they genuinely need the information they're requesting? If you're not quite sure about the validity of the email, don't hesitate to call or speak to the alleged sender. A quick chat can clear up any confusion.

Finally, if you receive a suspicious or threatening email, don't respond or click on any links. The best thing you can do is delete the email, but it may also be helpful to notify colleagues about the fake message in case they received it. ■

Brian Bosscher is the president and founder of Condo Control, a leading software company that provides web-based communication, management and security solutions for condos and HOAs of all sizes. He is also a board member, having served more than 12 years as both treasurer and president.
condocontrolcentral.com