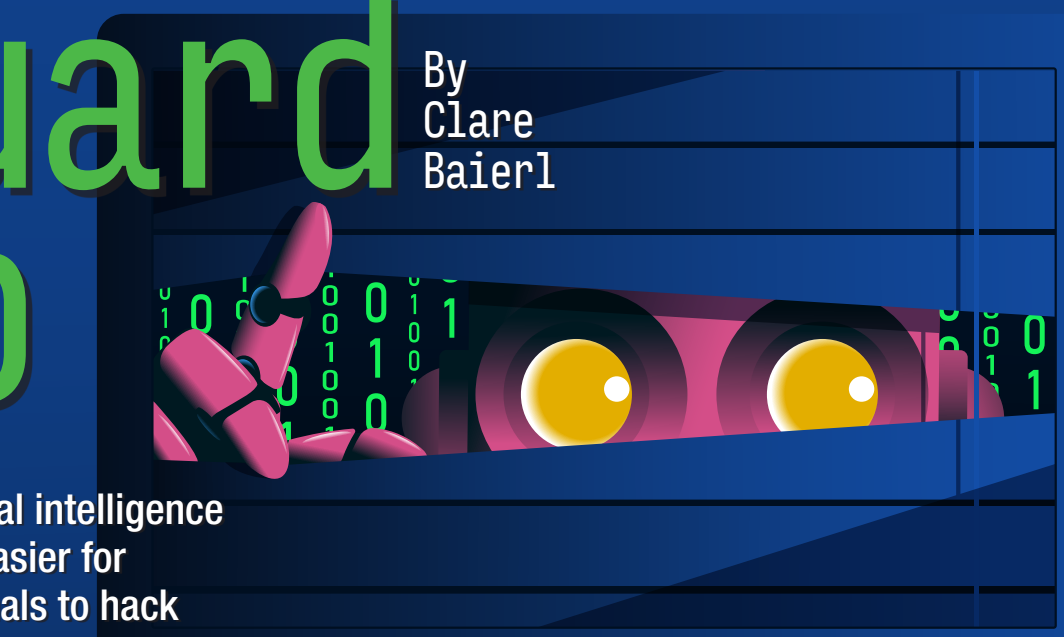
Get Your Guard Up

By Clare Baierl



With artificial intelligence making it easier for cybercriminals to hack into your accounts, experiencing a breach isn't a question of if but when. You can take steps to minimize your risk.

Not long ago, it seemed as if online scams were relatively easy to recognize and avoid. But that is no longer the case thanks to artificial intelligence, which is enabling hackers to carry out cyberattacks more easily and more quickly than ever before. And one of the prime targets of scammers? Co-op and condo communities.

A condo in the tri-state area became one of the latest victims of this increasingly prevalent problem when a board member's email account was breached by a hacker using AI-generated malicious code. The hacker, who noticed a recurring monthly invoice for the building's landscaping services, used the board member's email account to contact the property manager, informing him that the landscaping company had changed its banking information. When the next month rolled around and the property manager sent payment to what he believed was the landscaping company, the money went right into the hacker's

SHUTTERSTOCK/MOOR STUDIO

bank account. It took two months for the missing payments to be noticed, and by that time the hacker had disappeared without a trace. "This was a classic social engineering scam, which is when a hacker gets into someone's system and then dupes another party into paying them," says Ed Mackoul, the CEO of Mackoul Risk Solutions. "That was $60,000 down the drain."

One of the primary ways cybercriminals are leveraging AI is to increase the efficacy of phishing emails. Traditionally, hackers would have to meticulously write such emails, often posing as reputable companies, in order to trick people into granting access to their computers. But now, AI allows hackers to generate personalized emails almost instantly.

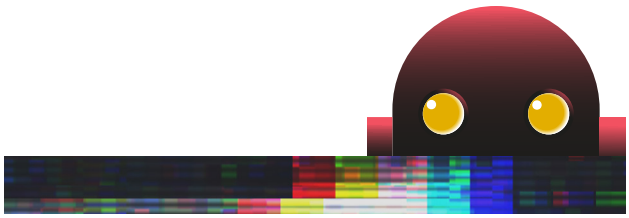
A midsize Manhattan co-op fell victim to this scheme when a board member clicked on a malicious link in a phishing email. The board member was in the process of reviewing a prospective buyer, and the hacker gained access to all the computer's information, including the prospective shareholder's personal information. While it was unclear what the hacker did with the information, the prospective buyer, upon learning about the exposure, sued the board, and it was forced to pay a settlement.

TAKING HOSTAGES

Encrypting information on a victim's computer and blocking access to it until a ransom fee is paid used to involve teams of people and hours of work, but it now can be completed in a fraction of the time by a single hacker using AI. Ransomware can strike many different kinds of computer systems, including a property's access system. One large co-op that had electronic building keys learned this the hard way. The hacker breached the property's access system and was able to prevent tenants from entering and leaving the building. The hacker demanded a ransom. Within two hours the property manager paid it through bitcoin — a cryptocurrency that enables attackers to receive payments that are difficult to track — and the system was back up again.

"These AI ransomware attacks are going to make the cyber landscape much more nightmarish," says Tanvir Arafin, an assistant professor at the George Mason University Department of Cyber Security Engineering.

AI ransomware can literally hold computer systems — and even residents — hostage.



PLACING BLAME

New York enacted the SHIELD Act in 2019, which strengthened the state's data security laws and added additional responsibilities to companies in the event of a security breach. For boards, this means maintaining reasonable safeguards to protect the security and confidentiality of private information. It also means that if there is a security breach, the affected party must be notified. Failure to comply with these requirements could result in fines of up to $250,000.

If a breach does occur and the affected party chooses to sue, the board is likely to be named in the lawsuit and will have to defend itself. "The general rule is that if you're suing and you're not quite sure who's liable, you sue everybody," says Mark Axinn, a partner at the law firm Phillips Nizer. And even when boards are not found responsible for damages, simply being named in a suit "could still run up a substantial legal bill," Axinn adds.

BEST DEFENSE

Many boards contract with third-party vendors that hold lots of secure information a building

uses. Your building could be working with companies like BoardPackager, which contracts with property management companies to handle the information needed to process residential real estate transactions, or BuildingLink, which offers software and hardware solutions that provide a myriad of modules to enable communication and tracking within your property. You'll want to make sure that any company your building contracts with maintains its own cyber liability insurance policies, with the board listed as an additional insured. Because your building's general liability and directors and officers policies don't protect against loss due to security breaches, you'll want to consider adding a cyber policy that includes both first-party coverage for the co-op or condo as well as third-party coverage for lawsuits resulting from breaches of another entity.

Cyber liability insurance is relatively inexpensive — typically around $1,000 a year — but premiums are on the rise due to an increase in social engineering claims by co-ops and condos. Reducing risk will make cyber liability insurance more affordable. "The more preventative measures you have, the better the chances that your rates could be lower," says Mackoul, the CEO.

In addition, it's important to shop around for a good policy. "Don't just take the first policy you're offered, because a lot of companies will try to put exemptions in that won't cover some breaches," says Sara Jodka, a member at the law firm Dickinson Wright who specializes in data security.

Training and educating board members to recognize phishing is a good place to start. There are free online courses that provide an overview and safety tips, such as Discover Threat Actors and Secure Your Digital Assets, offered by Salesforce via Trailhead at (https://bit.ly/DigSecCourse). Additionally, boards should never collect unnecessary personal information from residents and prospective buyers, and there should also be strict confidentiality procedures for all information received. Sensitive data like social security numbers, for example, should always be hidden from board members. Jay Hack, a partner at the law firm Gallet, Dreyer & Berkey who specializes in security, recommends that boards appoint a committee of two to three members to go through financial documents and summarize relevant information for the rest of the board. In addition, boards should not hold on to documents longer than needed. They should have a policy where all information that is no longer needed is disposed of after a set length of time.

As online threats are predicted to grow, it's more important than ever to protect yourself. "AI is very fast-moving, and we're always a little behind," says George Mason University's Arafin. "You need to have your guard up." ■