Grace Hill®

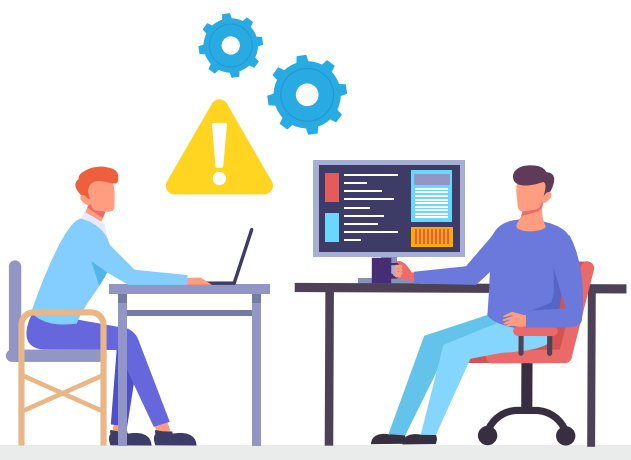
Cybersecurity for Office Workers

Cybersecurity is important because cyberattacks are a growing threat to business. These attacks can damage a company's reputation, financial bottom line, and operating ability. Businesses of all sizes, in all industries, and anywhere in the world are at risk.

The multifamily industry is an especially valuable target for cyberattacks because of the enormous amount of personal and sensitive information we hold, such as SSNs, birthdates, security question details, and previous addresses. One breach could be worth hundreds of thousands in damage (and more).

COST OF CYBERATTACKS

What's at stake? A lot, actually. In addition to the staggering statistics below, **60% of small businesses that experience a cyberattack go out of business within six months**.



4.24 MILLION
The average cost of a data breach in 2022

$6 TRILLION
Annual cost estimate of cyberattacks to the global economy

$170,000
The average cost of a ransomware attack

TYPES OF CYBERATTACKS

Cyberattacks come in many forms and fashions, with varying levels of sophistication. And unfortunately, it's likely not a matter of "if" your business will fall victim to a cyberattack but "when."

For that reason, it's essential to properly train (and test) staff to recognize the different types of cyberattacks. Knowledge is power. As employees learn what to look for — and truly begin to understand the potential financial and personal ramifications of nonchalance — you gain a vital partner in combatting these types of crimes.

Here's what to look for:

Phishing

Phishing is a type of social engineering attack. The attacker sends a fraudulent email or text message that appears to be from a legitimate source. The goal is to trick the victim into clicking on a malicious link or opening an attachment that contains malware.

Ransomware

Ransomware is a type of malware that encrypts the victim's files and demands a ransom payment in order to decrypt them. Ransomware attacks are often carried out through phishing emails or by exploiting vulnerabilities in software.

Data Breaches

A data breach is an incident in which sensitive, confidential, or protected information is exposed to an unauthorized person. Data breaches can occur through a variety of means, such as hacking, phishing, or insider threats.

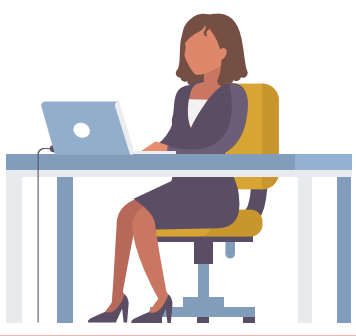
5 RISKY BEHAVIORS THAT THREATEN YOUR BUSINESS

Security is a culture, and your best defense is a solid offense because the bad guys are persistent.

Apple CEO Tim Cook said, "If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it."

5 RISKY BEHAVIORS TO AVOID*

1. **Clicking links or opening attachments in emails from unknown senders:** 43% of office workers have clicked on a phishing link in the past year.
2. **Downloading software from untrusted sources creates a vulnerability to ransomware:** 35% of office workers have downloaded software from an untrusted source in the past year.
3. **Allowing unauthorized access to company computers:** 25% of office workers have allowed unauthorized access to their company computers in the past year.
4. **Not keeping software up to date:** 35% of office workers do not keep their software up to date.
5. **Not reporting suspicious activity to IT:** 30% of office workers have not reported suspicious activity to IT in the past year.



HOW TO PROTECT YOUR BUSINESS

The most important determining factor in protecting a business is providing training and proper policies. Companies must adapt policies to fit their corporate structure, but cybersecurity training, in particular, cannot be considered "one and done." For optimum retention, training should be scheduled throughout the year to ensure knowledge is fresh and memorable for corporate and onsite teams.

However, there also are many practical ways employees can help protect their company from cyberattacks.

WHAT EMPLOYEES CAN DO TO PROMOTE CYBERSECURITY

- **Use strong passwords and change them regularly.**
- **Don't click on links or open attachments in emails from unknown senders.**
- **Keep software up to date.**
- **Be careful about what information is shared online.**
- **Report any suspicious activity to the IT department.**

By following these simple tips, office workers can help to keep their company safe from cyberattacks.

Cybersecurity is everyone's responsibility, and by working together, we can help make the internet a safer place for everyone.

But don't go it alone. Grace Hill can help you strengthen your cybersecurity muscle. Our powerful suite of solutions has comprehensive training and policy resources that support multifamily companies in beating the bad guys.

Need more help setting up cybersecurity policies and training?

Partner with Grace Hill to give your team the resources to know how to keep your company secure. Contact us today!

*Verizon Data Breach Investigations Report 2022