Millers Mutual

7 Cybersecurity Tips for Landlords

As a landlord, your properties may be made of bricks and mortar, but some of your most valuable assets aren't tangible.

Increasingly, rental property enterprises rely on digital systems and data to manage day-to-day operations and serve tenants. That means a cyberattack or accidental data loss could result in costly interruption to business, litigation, and reputational damage.

In fact, cyberattacks are an average of 2.5 times more costly than burglaries, yet many business owners still don't take digital security as seriously as physical security.

The good news is that you can significantly reduce your risk exposure by implementing these seven best practices:

1

Make a Plan and a Policy

Don't leave cybersecurity and responsible data usage to chance. Be proactive and craft a thorough written plan that guides your business operations, as well as a policy for your tenants.

Your cybersecurity plan should indicate what kinds of sensitive data you store and transmit, who can access it, how it's protected, and how you'll respond in the event of a data breach or loss.

Your tenant policy should include prohibitions on giving others access to the network and draining bandwidth by running servers or sharing files on peer-to-peer networks.

2

Use Strong, Fresh Passwords

Just like you wouldn't use "1234" as a keypad code to secure a building, you should create hard-to-guess passwords for all your networks and accounts – and update them regularly.

The U.S. Department of Homeland Security recommends that passwords be random strings of letters, numbers, and symbols at least 16 characters long, like tTc0evpr$Ytt@1ss.

Since these may be hard to remember, the experts suggest using a password manager program that functions like a master key – one strong password unlocks them all.

As an added layer of protection, enable multifactor authentication with an app that sends a time-limited code to your phone upon login.

3 Safeguard Your Wi-Fi Network

Wireless internet offers convenience and speed, and landlords often provided it as a free or discounted amenity to tenants. But Wi-Fi is a hacker's playground if the right safeguards aren't in place.

First, avoid connecting to public networks when you're working off-site. Anyone on the same network could potentially intercept the data you're transmitting.

Second, secure your own Wi-Fi router by disabling SSID (so your network won't be publicly visible) and enabling WPA3 (so your data is strongly encrypted).

4 Perform Regular Backups

The loss of valuable and sensitive data – like lease agreements, financial records, and maintenance logs – can happen due to a cyberattack, physical theft, power surge, or system crash.

Many experts recommend backing data up on at least one local device and at least one secure cloud storage service. That way, you can retrieve lost data from anywhere.

When you're busy running your rental business, it's easy to forget to do this, so set it and forget it by scheduling automatic backups on at least a weekly basis.

5 Update Your OS and Software

Your computer's operating system (Windows or macOS) contains critical built-in security features that protect against vulnerabilities and bugs, so it's important to enable automatic updates.

Likewise, make sure that you're running the latest versions of your firewall and antivirus software. These proprietary tools are constantly being enhanced to respond to the latest threats.

6 Choose Secure Payment Systems

Tenants appreciate being given an array of payment options, and many landlords enjoy the ease of sending and receiving digital payments. But it's best to steer clear of peer-to-peer apps.

P2P apps aren't designed for rent collection or other business transactions, and they may not offer the same protections and features that dedicated rent payment platforms provide.

These apps can also be more prone to human errors, like entering incorrect recipient information, and if disputes arise, it can be difficult to recover misdirected funds.

7 Defend Against Social Engineering

It used to be that cybercriminals mainly targeted big corporations with elaborate hacking operations. More and more, they're targeting small businesses through social engineering.

These schemes combine social and technical skills to gain a victim's trust and get them to reveal sensitive information or download a file that infects your computer with malware.

Phishing emails are an all-too-common form of this scam. The message might look like it's from a tenant, your bank, or another known party, but it's really a crook in disguise.

The best policy is to verify all requests for money or sensitive info by contacting the sender at a known address or phone number – not by replying or clicking a link.

Be Prepared. Get Covered.

The tips we've shared above will help you defend against both bad actors and bad luck. But when it comes to digital dangers, no business is invincible. That's where insurance comes in.

Learn more about Data Response & Cyber Liability Insurance from Millers Mutual, download our free fact sheet, and request a quote today.