HAI Group®

Five Cybersecurity Tips
For Affordable Housing Organizations

JONATHAN HOCHMAN,
Hochman Consultants

Protecting yourself from cyber criminals doesn't have to be complicated—or expensive. No single defense is perfect, but, taken together, these five tips from cybersecurity expert Jonathan Hochman of Hochman Consultants will go a long way toward helping your organization stay safe.

INVENTORY YOUR SYSTEMS

Do you have a list of every computer your organization has? Every scanner? Every router? Knowing what you have is critical, because every device, from your webcams to the internet-enabled locks on your doors, runs on software that gets updated periodically, mainly to fix known vulnerabilities. The first step to keeping yourself protected is knowing what you've got.

BONUS TIP : *Make sure to change the default passwords that came with your devices.*

PATCH YOUR SOFTWARE

Companies regularly issue software updates to fix problems that are discovered after a product release. Since most of these updates, or patches, pertain to security vulnerabilities rather than functionality, it's important to patch your software whenever there's an update.

BONUS TIP: *Set your computer software to update automatically by going into your system settings and turning on automatic updates.*

SECURE YOUR EMAIL

Email hacking is a huge problem for public and affordable housing organizations because you have data that is valuable to criminals. Practicing good password hygiene is a simple but powerful defense. Use different passwords for different accounts, choose phrases that are easy for you to remember bur hard for others to guess, and enable multi-factor authentication.

BONUS TIP: *Use a password locker like LastPass to generate and store passwords for you.*

RETIRE OBSOLETE SYSTEMS

Obsolete systems may look harmless enough, but they're vulnerable because they're no longer receiving software updates, making them a possible vector into your organization. (See #1).

BONUS TIP: *Make sure you have a process in place to remove login credentials for employees who have left your organization. A surprising number of companies don't do this.*

CONFIGURE YOUR DATA TO BACK UP AUTOMATICALLY

Backing up your data to the cloud—servers that are accessed over the internet—is critical, because it allows you to easily restore your files if you're attacked. A service like Microsoft One Drive will do it for you automatically.

BONUS TIP: *Practice restoring your data so that when you're inevitably hit, you've got a process in place to get back online quickly.*

NEED MORE GUIDANCE?

Visit **resources.haigroup.com/cybersecurity-center**

Be sure to review your cybersecurity insurance policy with your **insurance professional.**