RENTAL MANAGEMENT

FEBRUARY 2023

SAFETY POSTER

Types of cyber emergencies

Security breach:
92% of malware is delivered via email.
Source: Strong DM

Natural disaster:
75% of small business owners do not have a written disaster recovery plan.
Source: Webinar Care

Theft:
51% of small businesses admit to leaving customer data unsecure.
Source: Digital.com

Loss:
46% of breach victims are small businesses — with fewer than 1,000 employees. In 2021, this number grew to 61%.
Source: Strong DM

Unplanned downtime:
It can cost an average of $5,600 per minute.

98% of organizations say a single hour of downtime costs more than $100,000.
Source: Gartner

Human error:
88% of data breach incidents are caused by employee mistakes, according to Tessian — a security firm. Similar research done by IBM Security puts this number at 95%.
Source: Stanford University and Tessian study

Small businesses — with fewer than 100 employees — experience 350% more social engineering attacks than those at larger companies.

Social engineering attacks include phishing, baiting, quid pro quo, pretexting and tailgating. They rely on human interaction and psychology to get targets to break normal security rules and practices.
Source: Strong DM

34% of workers share their passwords with their colleagues.

Source: Techopedia

Password sharing is not the only issue, according to Survey Monkey:

- 22% of people surveyed admitted to reusing passwords on multiple work accounts.
- 58% say that they memorize their passwords; 34% write them on paper.
- 1 in 10 workers have a document on their computer full of passwords.