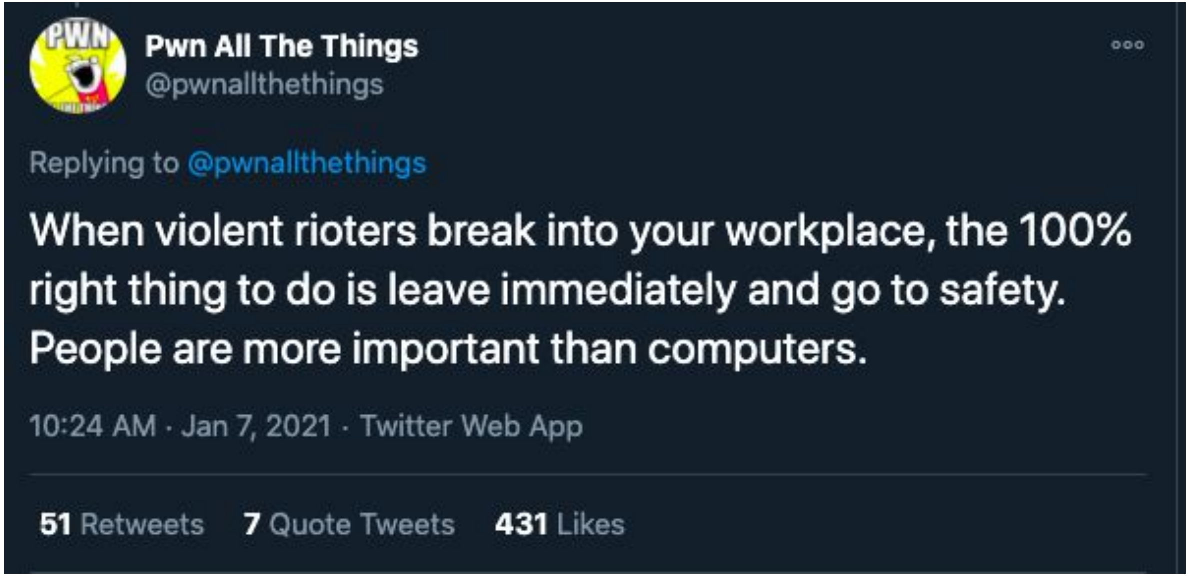
digital defense fund

Emergency IT Security:

Preparing and Protecting Your Office

Last updated 1/20/21



Pwn All The Things
@pwnallthethings

Replying to @pwnallthethings

When violent rioters break into your workplace, the 100% right thing to do is leave immediately and go to safety. People are more important than computers.

10:24 AM · Jan 7, 2021 · Twitter Web App

51 Retweets **7** Quote Tweets **431** Likes

Our Device & Network Security Goals

- If someone steals a laptop or phone, ensure it’s useless to them
  - Disk encryption
  - Strong unique password protection
- If someone gains unauthorized access to your office, ensure they can’t access your network
  - Strong unique wifi/network password protection
  - Autolock for computer screens

Our Device & Network Security Goals

- If someone steals a laptop or phone, ensure it’s useless to them
  - Disk encryption
  - Strong unique password protection
- If someone gains unauthorized access to your office, ensure they can’t access your network
  - Strong unique wifi/network password protection
  - Autolock for computer screens

In summary: if you have to leave your office on short notice, you can focus on your people and their safety, knowing that the sensitive information you steward is safe by default.

IT Preparation

These tasks can be implemented by individuals in your office, or at the network level if available. Coordinate with your operations or IT lead or related role:

- Full disk encryption
- Auto-lock on screens
- Keep your devices and software updated
- Know where to go to end active sessions (log out):
  - For your email
  - For your password manager
  - For other key accounts
- Back up essential data on a regular cadence

IT Fire Drills

- Lock your computer whenever you step away from it
  - Some computers have a "hot key" or shortcut to do this - google your model of laptop and "quick log-out"
- Practice ending sessions on your desktop/laptop from your phone
  - This can vary by email service or other software service
  - This will often look like "log out of all other sessions" under a privacy or security section of the email service on your phone
- Know how to access off-site backups.
  - Make sure you or your IT team make backups of essential data.
  - These backups should be stored off-site (physically or in the cloud).

IT Fire Drills

Look through the eyes of an intruder:

- Walk through the office after hours, or during a drill, and look around.
- What items, documents, devices are left out on desks? Which items are sensitive and can be moved into lockable storage when not in use?
- What document storage or filing cabinets are accessible? Can sensitive documents be moved into locking cabinets?

Questions to ask your IT team:

- Can we enforce auto-lock on screens in the office?
- Can we lock devices remotely?
  - If not: can we force logouts from important accounts remotely?
- Can we enforce full disk encryption on computers and phones?
- Can we auto-update devices and their software?
- What protocols are in place for IT infrastructure/devices if we need to evacuate the office?
- What protocols are in place to ensure devices have not been compromised in the case of unauthorized access?
- How often do we back up essential data? Where is it stored? How can I access it?