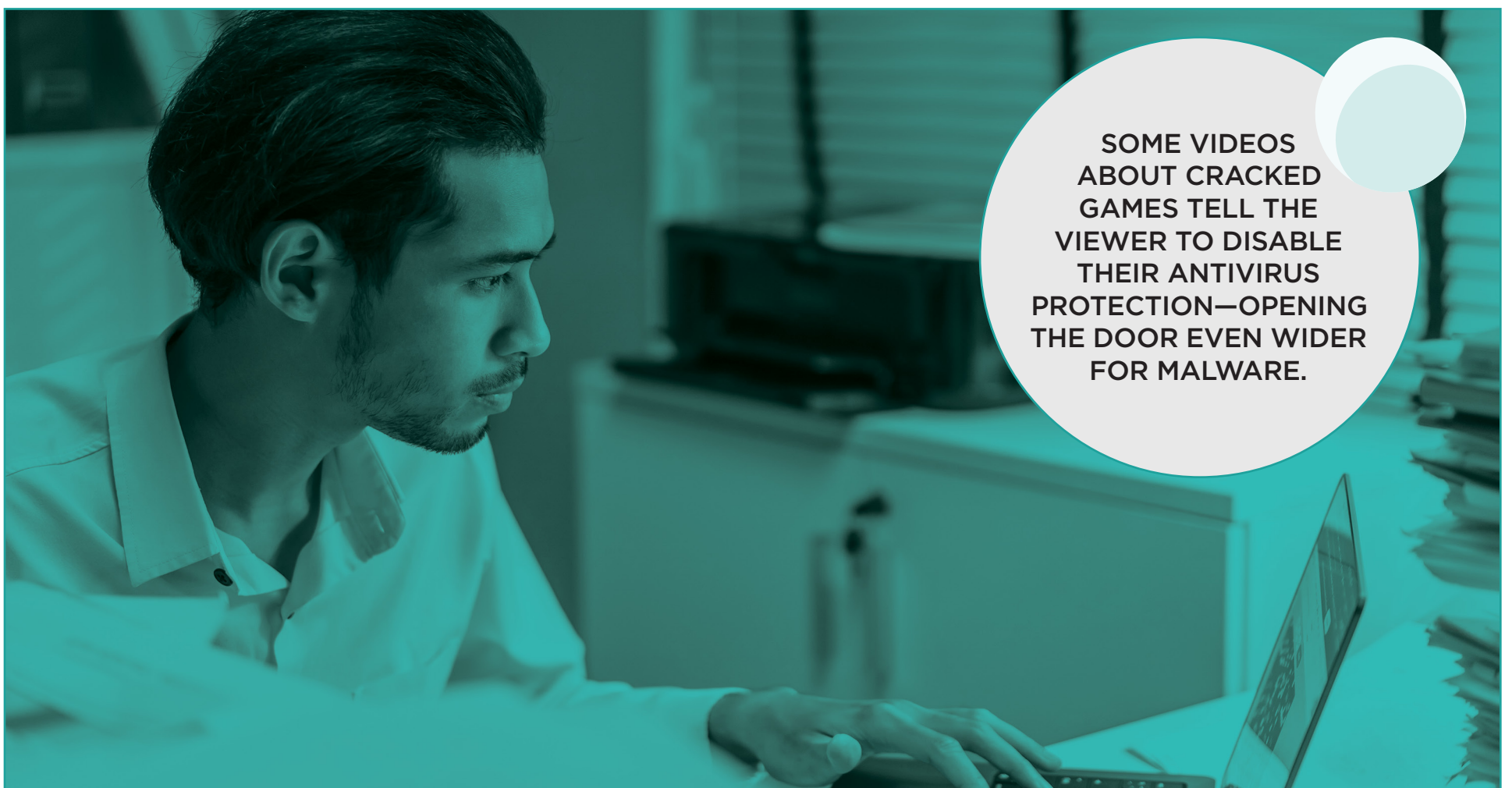# ATTACK
SPOTLIGHT

SHINING A LIGHT ON THE LATEST SECURITY THREATS

YOUTUBE MALWARE

Cybercriminals are posting videos to YouTube that promise to show you how to download pirated software or upgrade video games for free. But their real purpose is to trick people into clicking malicious links in the video descriptions.

These links lead to dangerous malware. Once a device is infected, the malware can steal the victim's login credentials and other data—and send it to the attacker.

SOME VIDEOS ABOUT CRACKED GAMES TELL THE VIEWER TO DISABLE THEIR ANTIVIRUS PROTECTION—OPENING THE DOOR EVEN WIDER FOR MALWARE.

Here are some tips for avoiding a YouTube malware attack:

- Don't download any type of pirated content
- Don't click on links in video descriptions—unless you are certain they are safe
- Avoid interacting with .exe and .rar files since they are frequently used for malware
- If you suspect a malware infection, report it immediately to the appropriate people in your organization