

# KNOW YOUR THREATS

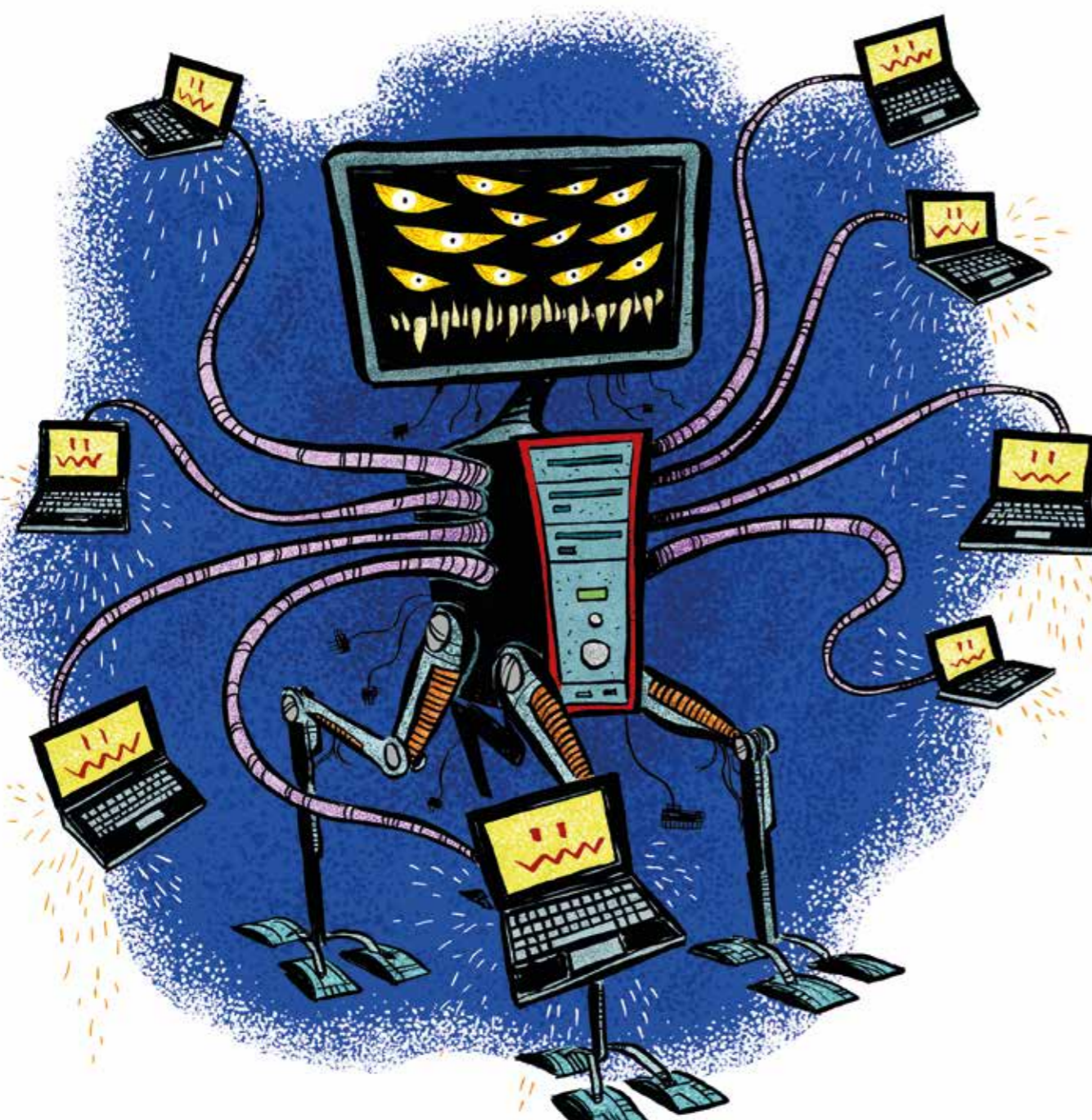
## RANSOMWARE

Ransom malware holds your data or system hostage until you pay up.



## BOTNETS

Networks of computers secretly controlled by an attacker, botnets will turn your devices into weapons for DDoS attacks.



## MALSPAM

Malicious spam is one of the primary methods of malware infection; it combines sneaky tactics and social engineering to hide malicious links or attachments within the email, tricking users into infecting themselves.



## TECH SUPPORT SCAMS

Tech support scams lure you with urgent messages of (fake) infection and demand you pay them to fix the problem.



## TROJANS

Trojans trick you into thinking they're legit but, once inside your system, unleash malware hell.



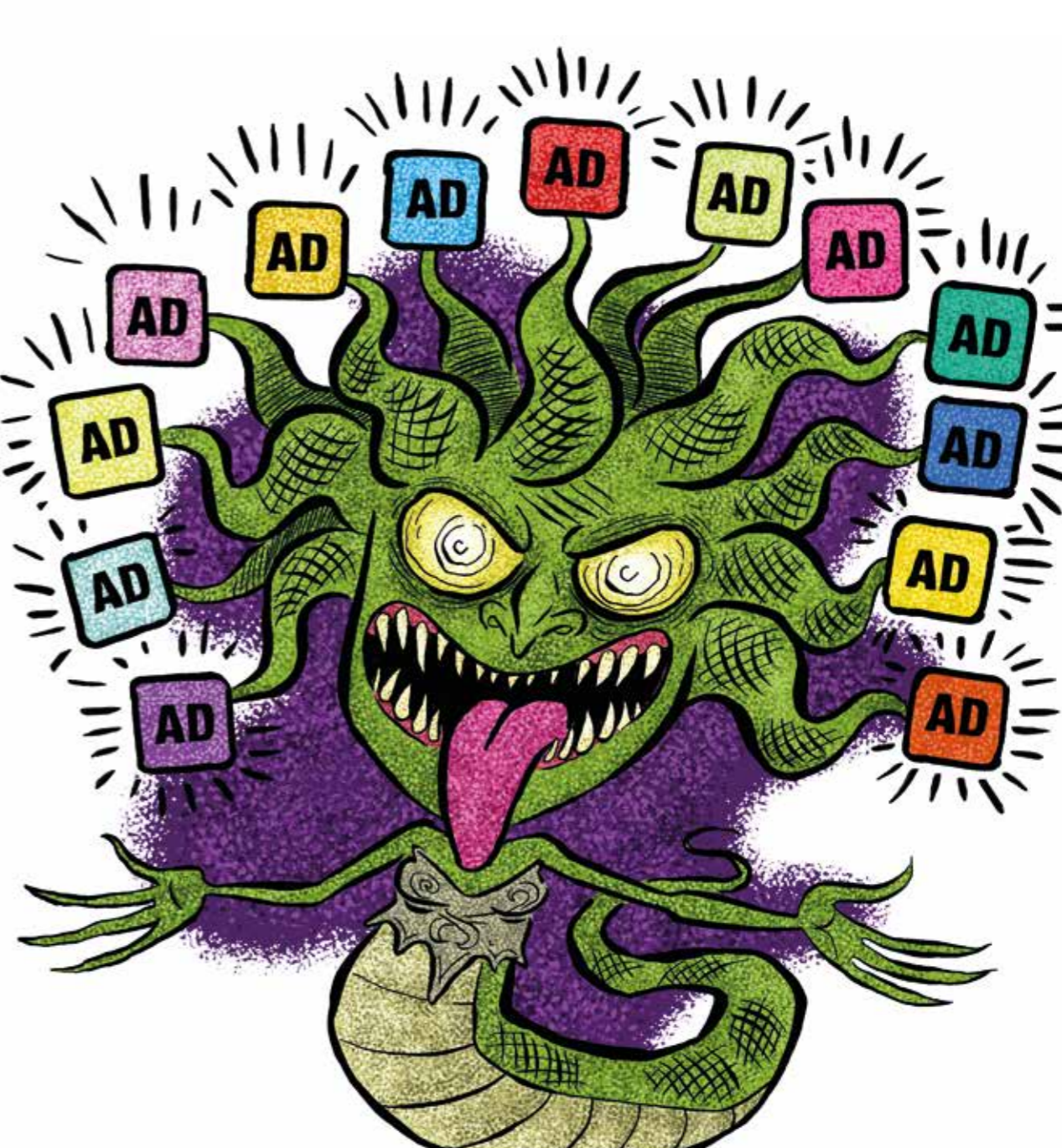
## SPYWARE

Sneaky spyware collects your personal information without you knowing, selling it on the black market or using it for future attacks.



## ADWARE

An annoying unwanted guest, adware bombards your device with advertising pop-ups, toolbars, and redirects to websites you didn't intend to visit.



## BANKERS

Banker malware focuses on stealing financial data like credit card numbers, bank login credentials, and other data, sometimes directly from forms you fill out in your browser.



## EXPLOIT KITS

Exploit kits look for holes in your system, taking advantage of the weaknesses and delivering malware when they find them.

