Ransomware
Holds your data or system hostage until you pay up.

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

Tech Support Scams
Lure you with urgent messages of fake infection and demand you pay them to fix the problem.

Adware
Bombards your device with advertising pop-ups, toolbars, and redirects to websites you didn't intend to visit.

Spyware
Collects your personal information without you knowing, selling it on the black market or using it for future attacks.

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

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

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

To learn more about malware and other threats, go to blog.malwarebytes.com