Innovation Growth Partners Specialty®

CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Cryptojacking Explained

Cryptojacking is a type of cybersecurity attack where hackers secretly hijack your computer's (or other device's) processing power to mine cryptocurrency without your permission. They achieve this by injecting malicious code, often through infected websites or malicious email attachments, to execute hidden mining operations. The victim bears the cost of the electricity and computing resources, while the attacker profits.

How Cryptojacking Works

1. Malware/Script Deployment
Attackers either infect a device with malware or inject a malicious script into a website.

2. Hidden Execution
When a user visits the compromised website or opens the infected file, the script runs automatically in the background without the user's knowledge.

3. Resource Hijacking
The malicious code uses the victim's device's CPU and other processing power to perform the complex calculations required to mine cryptocurrencies.

4. Profit for the Attacker
The cryptocurrency earned from these operations goes directly to the attacker.

Signs of a Cryptojacking Attack

Poor Device Performance
Your device runs slowly, crashes frequently, or exhibits unusually poor performance.

Increased Fan Activity
Your computer's fans are running faster and more often than usual to prevent overheating.

Overheating
Your device feels significantly hotter than normal, indicating excessive resource usage.

Rapid Battery Drain
For laptops and mobile devices, the battery drains much faster than it normally would.

High Resource Usage
You might observe unusually high CPU or memory usage in your system's task manager, even when only a few programs are running.

How to Protect Yourself

Keep Software Updated
Regularly update your operating system, antivirus software, and browser to patch vulnerabilities that cryptojackers might exploit.

Use Security Software
Install and maintain reputable antivirus and anti-malware software to detect and block malicious code.

Be Cautious Online
Avoid clicking on suspicious links or opening attachments from unknown sources in emails.

Use Browser Extensions
Consider using browser extensions or other tools that block cryptojacking scripts from running in your browser.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com