


Which Type of Cyber Threat Are You?

a Cybersecurity Awareness Month quiz brought to you by **CRITICALSTART** 

Ransomware, killware, phishing – oh my! There are many ways a threat actor can take advantage of your business or data. Protect yourself and your organization with multi-factor authentication, strong passwords, software updates and phishing reporting – and find out what type of cyber threat you are!

Question 1 – What's your biggest motivation?

- A. Money, money, money
- B. Winning, no matter who gets hurt
- C. Getting what I want by tricking people

Question 2 – Which best describes you?

- A. I'm all about the Benjamin's
- B. I like to live on the wild side and don't mind some chaos
- C. I love playing jokes and pranking people

Question 3 – What's your favorite movie genre?

- A. Crime
- B. Horror/slasher
- C. Comedy/dark comedy


Question 4 – What's your dream job?

- A. Financial analyst/advisor
- B. Doctor or surgeon
- C. Professional impersonator

Question 5 – What's your favorite color?

- A. Green
- B. Red
- C. Yellow

Which Type of Cyber Threat Are You?

a Cybersecurity Awareness Month quiz brought to you by **CRITICALSTART** 

If you got mostly **A's**, you are **Ransomware!**

Ransomware occurs when the threat actor holds personal data hostage or threatens to make it public, unless a ransom is paid. Infections usually start with an email with attackers hiding malicious website links in emails or other files. Because it's literally "where the money is", [financial services institutions](#) are a big target with a 1318% increase in ransomware attacks on banking in 2021.

If you got mostly **B's**, you are **Killware!**

The name sounds pretty scary, but for good reason. The main objective of killware is to cause physical damage or loss of life. The attackers behind this type of ransomware target human life, holding systems or files hostage or shutting them down. [Healthcare institutions](#) are a big target because of the devastating consequences of systems being taken over or shut down.

If you got mostly **C's**, you are a **Phishing Email!**

[Phishing emails](#) are digital communications sent to trick a user into giving up personal information or credentials. Attackers usually target individuals, looking for Personal Identifiable Information (PII) or credentials to access data/networks. Phishing emails often trick users by looking like they're from a company they know/trust and include a story to trick users to click or open an attachment, such as a free offer or saying there is an issue with your bank account.