

# Ecommerce assignment



**ASSIGN  
BUSTER**

Unit 5 Assignment Commerce Signs Your E-Commerce Website has been hacked If visitors report getting viruses from your web pages If visitors report being redirected to other websites If your search engine displays a warning “ This site may harm your computer” If your traffic decreases dramatically and suddenly If your files contain code you didn’t put there If your site contains files you didn’t put there If your search engine result page (SERP) listings suddenly change Damages that could occur if your site is hacked If a hacker is trying to hack your e-commerce site the disclosure of confidential data can occur.

Confidential data includes application specific data such as credit card numbers, employee details, and financial records. If your e-commerce site has been hacked you could experience damage some of the damage you might incur is the hacker could illegally use user accounts and privileges. After the attacker successfully gains access as a legitimate user or host, elevation of privileges or abuse using authorization can begin.

They could steal your hardware, steal software, run code to damage your systems, run code to damage, and corrupt your data, modify data that you have stored, steal your data, use your data for financial gain or for industrial espionage, perform actions that prevents legitimate authorized users from accessing network services and resources, perform actions to deplete network resources and bandwidth.

To protect your e-commerce site you could use encryption to secure pages when processing orders and payments. Use authenticated SSL certificates, so a visitor to your site will then have the assurance that you are what you

claim to be. Use digital certificates or business cookies because they will give you a unique Internet identity, like an ID or passport. Use anti-fraud solution to protect from Trojan horses, viruses, and worms.