Cyber attacks on education establishments can result in both direct and indirect costs – as demonstrated by these actual examples.

**DDoS:**
A DDoS attack occurs when a hacker takes control of thousands of computers and aims them at a single server, overwhelming that network with traffic and ultimately knocking it offline.

- **Costs:**
  - $3,000,000
  - Additional upgrades
  - Operational disruption
  - Reputational damage

**Ransomware:**
This is a type of malicious software, or malware, designed to block access to a computer system until a sum of money is paid to the person who unleashed it.

- **Costs:**
  - Approx $10,000
  - Operational disruption

**Phishing scam:**
Fraudulent email messages direct the recipient to a spoofed website or otherwise encourage the recipient to divulge private information that can be used to commit identity theft or fraud.

- **Costs:**
  - $cost of credit monitoring for 2000+ victims
  - Loss of employee confidence

**Targets**

- **College university:**
  Four attacks during a single school year.
  $3M spent on network security upgrade resulting in 2.3% raise in tuition fees.
  Upgrade failed to prevent another subsequent attack which brought down Internet/e-learning tools access.

- **Public school district:**
  Hackers blocked access to the district’s computer system using high-level encryption.
  Hackers demanded ransom payment via Bitcoin for the decryption key to release data.
  District officials paid the ransom after considering the time cost of restoring access with own resources.

- **School district:**
  A spoof email purportedly from the district Superintendent is sent to an employee.
  The email requests a list of employee names, addresses, salary details and Social Security numbers.
  The personal information of more than 2,000 employees is compromised.