## **Case study**

The staff at Sam's Scoops are excellent ice cream makers and make a product that is much loved in their seaside community; however, they know little about good online practices. Your task is to gather information on the do's and don'ts of online actions and then share your findings with the team. To be more specific, you'll identify **three vulnerabilities**, and for each one, you'll describe the **risk** it brings, the **type of attack** that a cybercriminal might use to exploit it, and a **mitigation** technique that can be used to reduce risk and improve safety.

## **Instructions**

### **Step 1: Identify plausible online threats**

Identify three potential threats that present a risk to a budding ice cream business looking to establish an online presence. Consider the types of online activities that small businesses tend to engage in. You can review the previous lesson content for ideas but expect to conduct some external research as well.

### **Step 2: Identify the risks posed by each threat**

Once you have figured out the threats, explain how each one can put the company at risk of an attack.

### **Step 3: Identify attacks used to exploit each threat, and their effects**

By which means might an attacker exploit each vulnerability, and how would the company be affected if an attack is carried out?

### **Step 4: Identify preventative measures relative to each threat that one can take to better protect the business**

Make Sam's team aware of what steps they can take to reduce vulnerabilities and better safeguard themselves against risks.

### **Step 5: Present your findings**

Write a summary of what you have found and consult the example below to understand how to format your report. Remember that you are presenting to an audience with limited knowledge of online dangers, so keep it simple and explain all unfamiliar terms. You can also support your explanations with images and diagrams as needed.

**Phishing Attacks:**

**[Vulnerability]**: Phishing attacks are a common online threat where cybercriminals attempt to deceive users into divulging sensitive information, such as login credentials or financial details.

**[Risk]**: **Impersonatation**

Small businesses often engage in email marketing campaigns or communicate with customers through email, making them susceptible to phishing attempts

**[Attack]**: **Theft of sensitive data / Reputation Damage**

Cybercriminals could impersonate the ice cream business in emails, directing customers to fake websites that collect their personal information, leading to identity theft or unauthorized access to the business's

accounts.

**Payment Card Fraud:**

**[Vulnerability]**: Ice cream businesses typically process online payments through their website or mobile app. However, this exposes them to the risk of payment card fraud. Vulnerabilities in the payment processing system to steal credit card information from customers during transactions.

**[Risk]**: **Data Breach**

If customers' payment data is compromised, the ice cream business may face legal liabilities, loss of customer trust, and potential damage to its reputation.

**[Attack]**: **Theft of sensitive data / Reputation Damage**

Cybercriminals could impersonate the ice cream business in emails, directing customers to fake websites that collect their personal information, leading to identity theft or unauthorized access to the business's

accounts.

**Distributed Denial of Service:**

**[Vulnerability]**: DDoS attacks are orchestrated attempts to overwhelm a website or online service with excessive traffic, causing it to become slow or unavailable. Small businesses, including ice cream ventures, might not have the sophisticated infrastructure to withstand large-scale DDoS attacks.

**[Risk]**: **Can not Function**

If the website crashed the ice cream business it could cause customers to go to another ice cream shop

**[Attack]**: **Reputation Damage**

attackers may target the ice cream business's website during peak hours or special promotions, disrupting online operations and resulting in revenue loss and customer dissatisfaction.

**[Mitigation]**: **Steps**

* Implement multi-factor authentication (MFA) and employee training to reduce the risk of falling victim to phishing attacks.
* Use secure payment gateways and comply with Payment Card Industry Data Security Standard (PCI DSS) requirements to safeguard customer payment information.
* Partner with a reputable web hosting provider that offers DDoS protection services, ensuring the website can withstand potential DDoS attacks.
* Regularly update and patch all software, including content management systems and e-commerce platforms, to minimize security vulnerabilities.
* Encrypt sensitive customer data and employ secure socket layer (SSL) certificates on the website to protect data during transmission.
* Create a clear and concise privacy policy that outlines how customer data is collected, used, and protected, fostering trust and transparency with customers.