10 ways to protect your business from online criminals

- [ ] **Train employees in security principles**
  Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail how to handle and protect customer information and other vital data.

- [ ] **Protect information, computers, and networks from cyber attacks**
  The best defenses against viruses, malware, and other online threats is to have up-to-date security software, web browser, and operating systems. Install other key software updates as soon as they are available.

- [ ] **Provide firewall security for your Internet connection**
  A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online.

- [ ] **Create a mobile device action plan**
  Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

- [ ] **Make backup copies of important business data and information**
  Regularly backup the data on all computers, automatically if possible, or at least weekly and store the copies either off-site or in the cloud.

- [ ] **Control physical access to your computers and create user accounts for each employee**
  Prevent unauthorized access to business computers by creating a separate user account for each employee and requiring strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

- [ ] **Secure your Wi-Fi networks**
  Wi-Fi networks must be secure, encrypted, and/or hidden. To hide your Wi-Fi network, set up your wireless access point or router, so it does not broadcast the network name and password protect access to the router.

- [ ] **Employ best practices on payment cards**
  Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

- [ ] **Limit employee access to data and information, limit authority to install software**
  Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

- [ ] **Passwords and authentication**
  Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry.