Tips for Safe Online Shopping

1. **Shop where you trust**
   When shopping in real life you will know the business and inventory exist. On the web, some businesses can be fabricated by people looking for your card information or other personal details. Consider purchasing only with retailers you trust and have shopped with before.

2. **Research the business**
   Do some research before you buy from a new merchant. Does the company interact on social media? Do they have positive customer reviews? Look at the Better Business Bureau – do they have a history of scam reports or complaints? You can even take it further by contacting the business. If you cannot find an email address, phone number or address for a brick and mortar location, that could be a warning sign that it's a fake company.

3. **Beware of deals that are too good to be true**
   If the website is offering something that seems too good to be true – then it probably is. Compare prices and pictures to similar website. Constant sales and low prices can be a sign that they do not actually have items in stock. This could be a fraudulent site trying to get your personal information.

4. **Avoid public Wi-Fi**
   With a little tech knowledge and the public Wi-Fi password available, a fraudster can intercept what you're browsing on the web. This can include, browsing history, emails or passwords. Online shopping usually means giving personal information a thief would love to have, including your name and card information. It is never a good idea to shop online or log in to websites while you are connected to public Wi-Fi. If you must purchase online while on public Wi-Fi, use a Virtual Private Network (VPN). This will create an encrypted connection between your device and the VPN server. Nearby hackers cannot intercept your information even if they have the Wi-Fi password.

5. **Online security**
   There are several things you can do to keep yourself safe online. Make sure your software and anti-virus protection is up to date. Updates often contain changes which help protect you and your devices from scammers and online criminals. Always choose strong passwords for your online accounts, using a combination of upper case, lower case, number and special characters. Using a phrase or sentence is good practice. Don't use the same password on multiple accounts. A data breach with one company could give scammers access to your other accounts that may share a password.

6. **How you can tell if a website is secure**
   Only ever put your card details into secure websites. Be on the look-out for the following signs to know you are shopping safely. Remember, this only means the site is secure, not that the seller is honest.

   Padlock symbol – There should be a padlock in the address bar next to the website address.
   Website address – This should start with https://. The S stands for secure
   Green address bar – On certain browsers and websites the address bar will turn green.
   Valid certificate – If you click the padlock symbol or just to the left of the address bar, you should see information on the site certificate. This should tell you who has registered the site. If you get a warning about a certificate, avoid the website.

7. **Don’t give out more information that needed**
   No shopping website should ever need your Social Security number. If you are asked for personal details, call the merchant’s customer service and ask if you can supply other identifying information or just walk away.

8. **Check your statements**
   Check your account statements monthly or monitor charges regularly through Internet or Mobile banking. Through Internet or Mobile banking, you can also set up custom account alerts to send a text or email to notify you of charges or balance changes.