ONLINE SHOPPING

Online shopping is gaining popularity as consumers increasingly seek convenience and benefit from price competition. However, online shoppers need to be aware of the common risks associated with purchasing goods and services on the internet:

- **Fake Websites** - They offer incredible deals that are hard to pass up and then disappear a few weeks later. Their sole purpose is to steal your personal information to be used in identity theft and hacking.
- **Unencrypted Sites** - Sites like this leave you vulnerable online; they enable anonymous people to track and obtain your information or even inject malware into the website.
- **Hidden Charges** - Shoppers should always check the final amount and fine print related to their online purchases to avoid paying more than expected. Sometimes sellers may include hidden charges, duties or shipping fees.
- **Scams or Fraud** - Some of the common complaints include buyers not receiving purchased items, received goods are either less valuable than or significantly different from what was advertised, and receiving fake coupons and gift cards for identity theft purposes.
- **Seller's Credibility** - The shopping site is not secure or showcases unknown sellers.
- **Safety Standard Issues** - The item you purchase may not meet SIRIM quality of safety standard.

So How Do You Shop Online with Confidence?

- **Protect Your Computer**
  Regularly update and protect your computer with anti-virus and anti-malware software.

- **Shop with Familiar Companies**
  Buy from companies that you are familiar with because anyone can set up a secure server.

- **Use familiar websites**
  Only use trusted websites by well-known companies or retailers.

- **Update browser**
  Make sure you update the browser to the latest version so that the information you send through it is secure.

- **Use a Secure Server**
  Before entering personal information, check out a few things. Look if the URL starts with https (not http) and that there is a padlock at the bottom of the website. Some browsers have the padlock right next to the URL.

- **Use Secure Passwords**
  Just because the account is used for shopping, doesn't mean it doesn't deserve secure passwords. Remember, your sensitive information is captured in the account.

- **Double Check**
  Double-check the address in the address window to be sure it is the site you want especially if you followed a link from an email (amazon.com should say amazon.com in the URL and not annazon.com or something else).

- **Avoid Up-front Payment**
  Avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.

- **Use Credit Cards**
  Debit cards don't offer you the protection of unauthorised use, like the one accorded to credit card holders. In most cases, you will only be held liable for minimal amount and you can protest a charge if you don't get what you ordered. For more info on liability of card holders on unauthorised charges, please contact Bank Negara.

- **Do a Thorough Checking**
  Before doing business with an unknown company:
  - Make sure there is contact information for the company (business name, address, and telephone number). Compare this with information from the domain register.
  - Check the company policy on payments and returning goods.
  - Check to see if there have been complaints filed with consumers' associations or the authority responsible for consumer protection.

- **Print and Keep Information About Your Order**
  Print out information (hard copy or pdf) on your order, the return policies, company information, specific product information, warranty information, and correspondences between you and the seller.

- **Consider Calling in the Order**
  If you don't feel comfortable entering your credit card information online, then call the company and place your order.

- **Check Statements**
  Regularly check your financial statements for any unauthorised transactions.

- **Trust Your Instincts**
  If it sounds too good to be true... it probably is!