FAQs for Safe Financial Transactions Online

1. **How to create a strong password?**

   Use a long password made up of numbers, letters and symbols
   The longer your password is, the harder it is to guess. So make your password long to help keep your information safe. Adding numbers, symbols and mixed-case letters makes it harder for would-be snoops or others to guess or crack your password. Please don't use '123456' or 'password,' and avoid using publicly available information like your phone number in your passwords. It's not very original, and it isn't very safe!

   Try using a phrase that only you know
   One idea is to think of a phrase that only you know, and make it be related to a particular website to help you remember it. For your email you could start with "My friends Akshay and Sheetal send me a funny email once a day" and then use numbers and letters to recreate it. "MfA&Ssmafe1ad" is a password with lots of variations. Then repeat this process for other sites.

2. **Is it safe to use public WiFi for financial transactions?**

   It's good to be extra careful whenever you go online using a network you don't know or trust – like using the free Wi-Fi at your local cafe. The service provider can monitor all traffic on their network, which could include your personal information.

   However, if you are using a service that encrypts your connection to the web service, it can make it much more difficult for someone to snoop on your activity.

   Avoid logging into accounts that contain sensitive financial information (e.g. bank or credit card accounts or commerce websites) on public or shared computers. If you do access such information on a public or shared computer, remember to sign out completely and close your browser window after you're done.

3. **How to check if the website is secure?**

   - First, look at the address bar in your browser to see if the URL is correct - watch out for typos (for instance, www.example.com is not the same as www.exaample.com)
   - You should also check to see if the web address begins with https:// – which signals that your connection to the website is encrypted and more resistant to snooping or tampering.
   - Some browsers also include a padlock icon in the address bar beside https:// to indicate more clearly that your connection is encrypted and you are more securely connected.

4. **How to check if a website is safe for online transactions?**

Look for the https:// connection in the address bar (and the padlock icon in your address bar if you're using Google Chrome or Internet Explorer) when transmitting any sensitive information like credit card or bank numbers.

When accessing financial accounts, check that the website has an Extended Validation Certificate — the URL or website name should show up as green in the URL bar of many modern browsers, meaning the organization that operates the website has been validated.

To manage financial transactions or shop on your mobile, install the official mobile application of your bank or the e-commerce platform you trust. To make sure you have the right application, check the official website or look at the user reviews.

5. **How can I keep my device free from malware to perform secure financial transactions?**

- Keep your browser and operating system up to date. Most operating systems will let you know you when it's time to upgrade – don't ignore these messages. Old versions of software can sometimes have security problems that criminals can use to easily get to your data.

- Keep an eye on what you click and download. Without meaning to, you may click a link that installs malware on your computer. To keep your computer safe, only click links and downloads from sites that you trust. Don't open any unknown file types, or download programs from pop-ups that appear in your browser. Also pay attention to the fine print details and any auto-checked checkboxes when downloading. Make sure that you understand what programs are being installed.

6. **Is it okay to provide personal information online during transaction online?**

Be careful anytime you receive a message from a site asking for personal information. If you get this type of message, don't provide the information requested without confirming that the site is legitimate. If possible, open the site in another window instead of clicking the link in your email.

If a site is asking for personal information beyond what is required to purchase a product or receive a service (e.g., bank account information, security question answers, or passwords) be suspicious as these types of inquiries may be indicative of a phishing attempt. Some sites may be a carbon copy of the official site, including logos and text, but are set up by fraudsters with the sole purpose of obtaining your personal information.

7. **How to check if an e-commerce site is genuine?**

If you haven't shopped from a merchant before, check beforehand to make sure they're legitimate. For example, learn more about their business history and do a web search for reviews from other buyers with experience with the seller.

Legitimate merchants should provide you with contact information that you can reference if you have any questions or problems with your transaction, which may include a physical address, contact phone number, or email address.

Many sites selling counterfeit products will have official sounding URLs, which might include phrases like [brand]onsale.com or official [brand].com. Checking the site's WhoIs record is one way that might reveal who owns the domain.

8. **What are the factors to check before purchasing online?**

- **Compare the price:** Compare what you're seeing with similar goods being sold elsewhere. If the price is significantly different, use caution - make sure to research the seller and ask questions about the condition of the item. When a site offers products that are heavily discounted, contains bad grammar and misspellings, and uses low quality images of the brand owner's official site, it might be selling counterfeit products. Be careful though, some sites selling counterfeit products mimic the brand owner's site by imitating the layouts and using similar images or using a domain name incorporating the brand.

- **Read the fine print:** Before you purchase, make sure you're familiar with the seller's shipping, warranty, and return policy. Some stores will offer full refunds, while others charge restocking fees and give only store credit.

9. **What are the steps to keep in mind after purchasing online?**

- **Keep a record of the transaction:** Having a digital or paper copy of large transactions can help you if you do need to make a return or contest unauthorized charges made to your account.

- **Make sure you got what you paid for:** Once you've received the item, give it a quick check to make sure everything is as it should be. The sooner you can try to address a case of fraud, the better chance you have to resolve it positively.

10. **What is Phishing attack and how to protect yourself from it?**

A phishing attack happens when someone tries to trick you into sharing personal information online. Phishing is typically done through email, ads, or by sites that look similar to sites you already use. For example, you might get an email that looks like it's from your bank asking you to confirm your bank account number.

Don't navigate to sensitive accounts by clicking a link or copying and pasting the address. Instead, type out the web address yourself. But make sure that you're inputting the correct address; some typosquatting sites look exactly like the real site, but are set up to phish your account information.