

# Protecting your financial information online

At Synergy, we are committed to protecting your personal and financial information, whether you are in branch or online, in the middle of a big city at a shopping mall, or in the middle of your field or an oil site. As such, we want to share some tips to keep you and your information safe online (as there are fraudsters who try to impersonate web pages or emails to access your personal information). One of the common ways fraudsters try to access your information is through an online scam called phishing.

## What is phishing?

Phishing is an attempt by cyber criminals to pose as someone you trust so you will reveal passwords and confidential information. The most common mode of phishing is through fraudulent emails or a fake link that directs you to a fake website (that looks very similar to the real website). An example of phishing could be fraudulent INTERAC eTransfer<sup>†</sup> emails that are designed to look real and ask you to provide your online banking information. Clicking on the link and entering any personal details could compromise your personal and financial information. The good news is there are ways to detect whether an email or link is real.

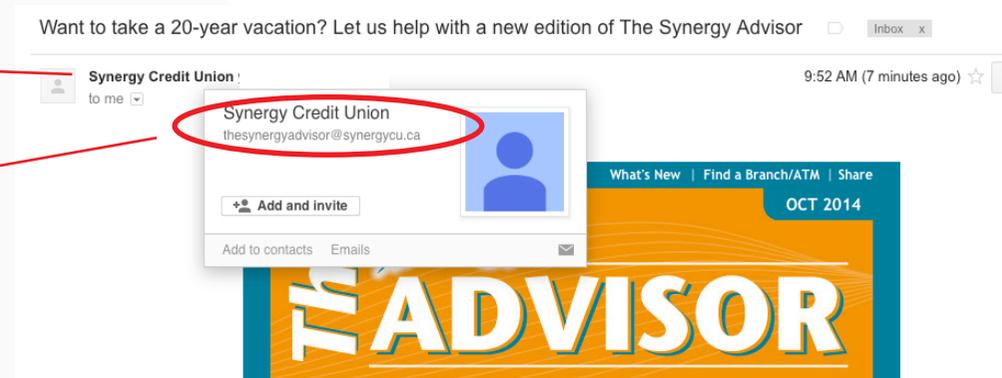
## How do you know if you are on the real Synergy Credit Union website and online banking?

One of the most important ways to protect your personal and financial information is to know when the email is real or know when you are on the real Synergy Credit Union website and online banking. These tips can help you know the difference:

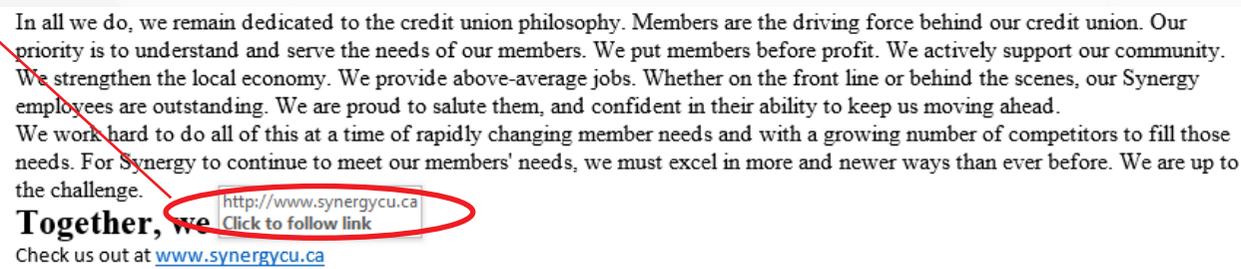
1. In an email, confirm the source of the email is accurate (needs [@synergycu.ca](mailto:@synergycu.ca) at the end of the email address). Hover over the email address to ensure it is the same email it shows. It should contain [@synergycu.ca](mailto:@synergycu.ca) at the end of the email address.

**Email from:**

**Email address appears when hovered over**



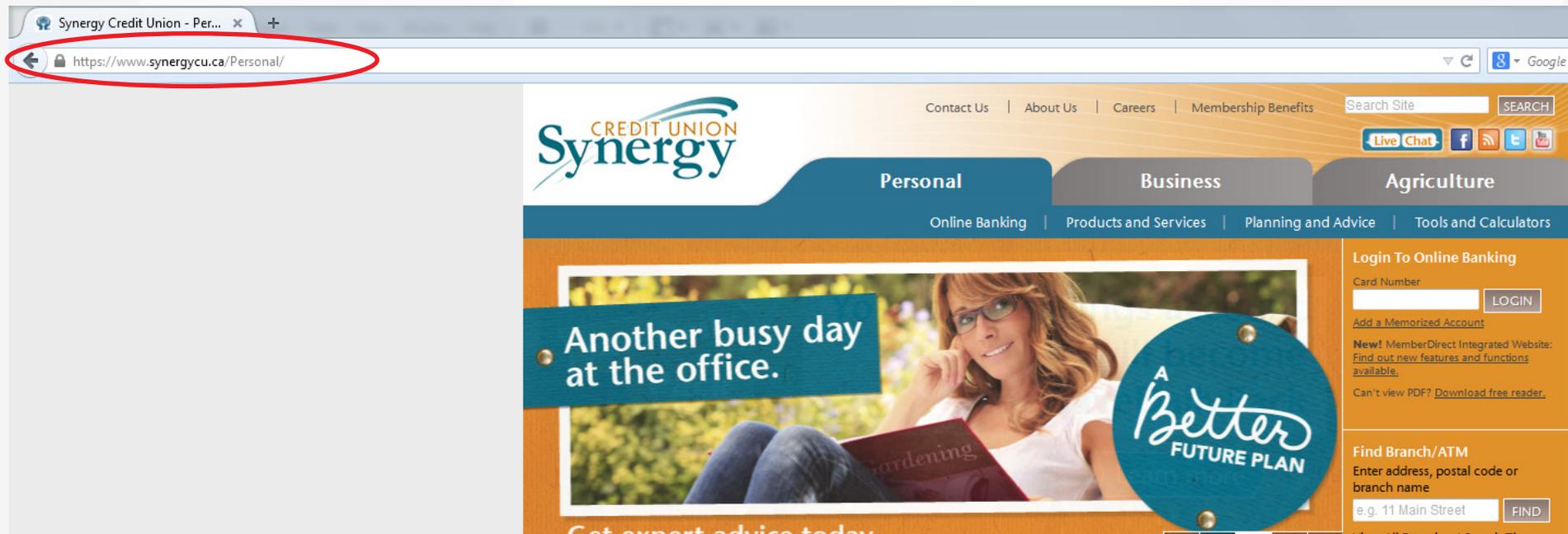
2. If you are clicking a link in the email, ensure the link includes [www.synergycu.ca](http://www.synergycu.ca). This can be done by hovering over any link to ensure it links to [www.synergycu.ca](http://www.synergycu.ca) and goes to the Synergy Credit Union website.



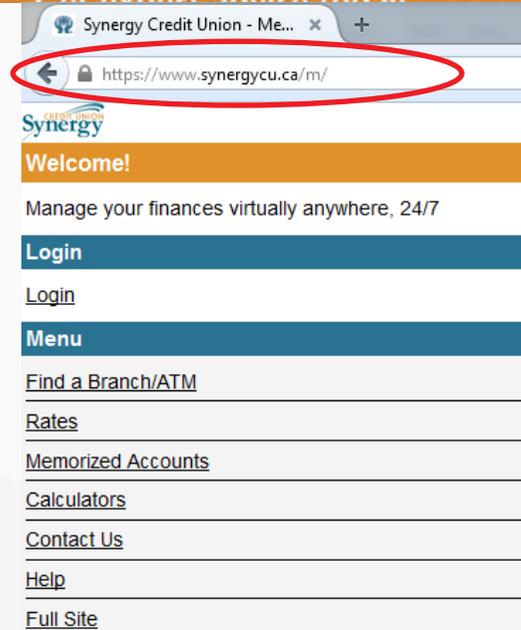
# Protecting your financial information online

3. When visiting Synergy's full version of online banking or the mobile web version in Mobile Web Banking, type in the web address yourself or ensure you are at the correct address by quickly looking at the web address in your web browser bar. If you are on the full version or the Mobile Web Banking version, the following web addresses would be found at the beginning of the web address:
- [www.synergycu.ca](https://www.synergycu.ca) (full version), or
  - [www.synergycu.ca/m](https://www.synergycu.ca/m) (Mobile Web Banking for browser-enabled devices).

**Full  
Version**



**Mobile Web  
Banking**



# Protecting your financial information online

4. After you enter your card number to access online banking, do not enter your password unless you see your security questions and/or personalized image. (This will verify it is your account, and then you can safely login.)

The image displays two side-by-side screenshots of the Synergy Credit Union online banking login page. The left screenshot shows the 'Security Question' step, where the user is asked, 'What is your maternal grandmother's first name?'. The right screenshot shows the 'Login' step, which includes a 'Security Image and Caption' section. A red arrow points from the caption text box to the 'Security Image and Caption' heading.

The caption below your image should show the previous phrase you selected when you signed up or updated your information within online banking. Synergy Credit Union will never ask you to update your personal information, or your security questions, image or caption.

Please note, on the Banking App, if you have a card number memorized using the 'Remember Me' function for quicker service, you will not see an image or question to verify the Banking App. You will just need to enter your Personal Access Code (password) to access your information. To ensure you are on the valid Synergy Banking App, please make sure you only download the Banking App through the Apple or Android stores where you originally downloaded or where you update your app. These stores verify the Apps are from a valid source or company. Only download the app from sources that can be verified.

# Protecting your financial information online

## Another popular phishing scam

Another example of a recent phishing scam is a fraudulent email that claims to be from the Canada Revenue Agency. This fraudulent email says taxpayers are entitled to receive a tax refund. The fraudulent email may ask the receiver to enter their personal information, or it may refer to them to a fraudulent site that looks the CRA website. At this site, they are asked to enter personal information to verify their identity. Entering this information could result in identity theft. According to the CRA's website:

- The CRA never requests, by email, personal information of any kind from a taxpayer.
- The CRA will never request information from a taxpayer pertaining to a passport, health card, or driver's license.
- The CRA will not divulge taxpayer information to another person unless formal authorization is provided by the taxpayer.
- The CRA will not leave any personal information on an answering machine.

Synergy Credit Union will also never ask for your financial information online. If you receive an email of this nature, contact the business source to confirm it is real.

## Extra tips to help protect your information:

- Check your account and credit card statements regularly and carefully to ensure all transactions are legitimate.
- Keep in mind we will never ask you for your personal passwords, personal information numbers or login information in an email. (This is the easiest way to tell if an email is fraudulent.)
- Download Banking Apps from Google PlayStore or the Apple App Store only (for our Android and Apple Banking Apps). These stores verify the Apps are from a valid source or company.
- Sign up for Security Alerts in *MemberDirect*® Online Banking. At Synergy, you can sign up to receive an alert by email or text when certain online activities occur in your account, such as when someone logs in or tries to set up a new bill or INTERAC eTransfer<sup>†</sup> payee.
- Make sure you have current virus protection on your computer. Virus protection can be purchased online or in stores. There are also free virus programs that can be downloaded online, such as AVG or Avast.
- Remember to protect your passwords and update them regularly (every 60 to 90 days).
- Update the operating systems on your computer, smartphone or tablet.

If you discover or suspect unauthorized activity has occurred in your account or if your password may have been compromised, please notify Synergy Credit Union immediately at 1.866.825.3301. You can also change your Personal Access Code (password) anytime at your nearest Synergy Credit Union ATM, through automated telephone banking or by contacting us.

Your personal and financial information, as well as your online security are important. To learn more about your internet security, visit: <https://www.synergycu.ca/Personal/AboutUs/OnlinePolicies/InternetSecurity/>. We're here to help.