Banking Safely Online

While banks do everything they can on to make sure you’re banking safely, you need to do your part too.

|  |  |  |
| --- | --- | --- |
| 1. | As best practice, type the web address directly into the address bar or use a search engine to find it.  **Never** follow a link to your bank from an email, as the email could be a **‘phishing’** scam. |  |
| 2. | If you are using a search engine, be sure to check the site you click through to the correct **URL** that is definitely your bank.  Cyber criminals sometimes create extremely convincing ‘spoof’ sites to get your log-in details. One thing they can’t fake, however, is the URL – so check it’s exactly right. |  |
| 3. | Once on the site, make sure there is a **padlock** symbol in the browser’s address bar the web address should change from beginning with “http” to “**https**”, indicating the page is secure.  A padlock on the web page isn’t enough because that can easily be faked – instead look to the left or right of the web address. |  |
| 4. | If your bank offers additional security software, such as NatWest’s Rapport, use it alongside your computer’s own **security software** for added protection. | |
| 5. | If you do notice any unusual or inexplicable transactions in your online statement, **contact your bank** directly by phone and query or report it. | |
| 6. | **Don’t ever share** your login details with anyone and if you use a shared computer for accessing your online bank accounts, don’t allow the browser to remember your log-in credentials when prompted. | |
| 7. | Finally, make sure you’re fully **logged out** before you leave your bank’s website. | |