How to avoid being phished

Never respond to emails that request personal financial information

You should be suspicious of any email that asks for your password or account information, or includes links for that purpose. Banks and ecommerce companies do not usually send such emails.

Look for signs that an email is "phishy"

Some phishing emails are generic, using greetings like "Dear valued customer." They may also include alarming claims (e.g., your account numbers have been stolen), use suspiciously poor spelling or grammar and/or request that you take an action like clicking a link or sending personal information to an unknown address.

Other phishing emails are more targeted and may be very believable. Look for unusual behavior, such as a blank or irrelevant attachment (which could have hidden malware), or a request to click a link that doesn't fit with the topic or sender of the message.

Visit bank websites by typing the address into the address bar

Don't follow links embedded in an unsolicited email. Phishers often use these to direct you to a bogus site. Instead, you should type the full address into the address bar in your browser.

Keep a regular check on your accounts

Regularly log in to your online accounts and check your statements. If you see any suspicious transactions, report them to your bank or credit card provider.