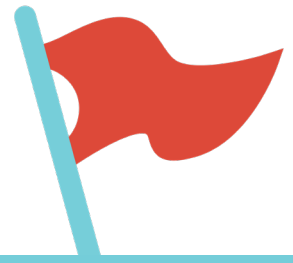


# Don't Get Spooked by Scams

Red flags to watch for when browsing the web



The threat of bank scams is ever-present on the internet. Scammers prey on vulnerable individuals and trick consumers into giving away their private information by using a variety of tactics. Learning how to identify fraudulent schemes and staying alert of possible scams will always be the first line of defense when battling bad actors. Below are a few common red flags consumers should look out for to avoid falling for an online bank scam.

## 1. Fraudulent Communication

Scammers will usually contact consumers unexpectedly via text, email, or other mode of online communication. Many schemes even include disguising phone numbers and email addresses to appear as credible senders from a bank. The message will often prompt the recipient with a call to action while seeking private information that will fix the issue. It's important to know that banks will never contact you to ask for personal information. When in doubt, call your bank to verify they contacted you.

## 2. Pressure to Act Immediately

Consumers often fall for victim to bad actors because their communications elicit panic and fear. Common bank scams often relate to issues that require immediate attention — such as suspicious activity or a hacked account. To address the concern, recipients are asked to click a link where they will need to provide private financial information. The links will even appear credible or almost identical to the bank or company. Once a scammer has a login or account information, they have control of the account.

### Helpful Tip:

If you use a mobile banking app, turn your notifications on to receive email or text message alerts any time money is withdrawn from your account.

## 3. Unsecured Web Address

Scammers find victims by placing banner ads on websites, sending mass emails, or setting up fake stores selling false products. Make sure the link is secure by finding the "s" in https:// in the beginning of the URL. A link with http:// is not secure. Consumers should also seek refund policies, terms and conditions, or contact information to verify a website's credibility. Only disclose account or login information when on the bank or company's valid website or mobile app. Being asked to pay using a non-traditional method of payment or money transfer is also a red flag.

## 4. Too Good to Be True

Be on the look out for any communication telling you that you won a cash prizes, irresistible product deals, pre-approvals, or free rewards. If it is too good to be true — it's probably a scam. Never provide financial information to collect a prize. Other red flags to be aware of while surfing the web include unsecured WiFi connections, false job advertisements, or even fake quizzes or games that ask for personal information. Always be skeptical when asked to provide private or financial information, especially if you didn't initiate the conversation.



If you fall victim to a scam, immediately contact your bank to freeze your accounts and the police to report the incident. Do not be embarrassed of falling victim to these increasingly sophisticated bad actors. It is better to act now than face greater consequences later.