SHARE:

Join Our Email List

View as Webpage

The Top Scams to Look Out for in 2023

In the digital age, it's important to remain vigilant against scams and fraud attempts. Unfortunately, scammers continue to find new and creative ways to trick individuals into giving away their personal information. By being aware of these scams and knowing how to protect yourself, you can help ensure your finances and personal information stay safe and secure. Learn about the 5 most common scams to be aware of in 2023 below.

Student Loan Forgiveness Scams

This is the most common form of a student loan scam, arriving via telephone, email or text message. Some of these may look legitimate, with forms to fill out sensitive information,

including banking account information and your Social Security number. **The Department of Education's student loan website** has a wealth of information on pinpointing student loan forgiveness scams and what to do if you become the victim of one.

Payday Loan Scams

Scammers will reach out to individuals either posing as a debt collector, wanting payments through gift cards or with an offer for a fake payday loan. Scammers will then steal sensitive information and/or steal the money that was placed on a gift card. For more information on payday loan scams, **read this report** from the Better Business Bureau.

Gift Card Scams

With this common scam, criminals will ask you to provide payment via a gift card, usually iTunes or Google Play. The **FTC warns** that gift cards should only be gifts and never be sent as payments. These scams may come to you via email, text message or phone call and may often pose as someone you know, such as a coworker, or may pose as a government institution.

QR Code Scams

QR codes are everywhere nowadays, especially in the contactless culture that has developed since the pandemic. Illegitimate QR codes will direct you to sites aimed at stealing your information. While these can't be pinpointed with the naked eye, never scan a QR code from an untrusted source. Always check the URL after you've scanned the QR to ensure the site appears legitimate. Learn more about QR code scams **here**.

Cryptocurrency Romance Scams

Online romance scams go back to the birth of the internet. Criminals are now using platforms such as dating sites or apps to commit their crimes, convincing you to download an app and contribute to a cryptocurrency fund that will grow their wealth. If you are approached with any investment opportunity, careful consideration is necessary. Here are some **additional red flags** that you may be involved in a cryptocurrency romance scam.

If you receive an unsolicited phone call or text message requesting your Oak Bank account information, report it immediately by calling 608.441.6000 or sending an email to bank@oak.bank.

Oak Bank will never ask for personal information over an unsolicited phone call, text, email, or online chat. Never share your account information, PIN number, username/password or one-time password.

For additional security information, you can visit Oak Bank's Security Information on our website.

Need help with your account?

Email: bank@oak.bank
Call: 608.441.6000

If your Oak Bank Debit/ATM Card has been misplaced, call 800.472.3272.

If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

Visit Oak Bank Online

608.441.6000
877.625.2265 Toll Free

Lobby
M - F: 8 a.m. - 5 p.m.

Drive-up
M - F: 8 a.m. - 5 p.m.

Member FDIC

STAY CONNECTED

This Oak Bank message may contain promotional content.