



YOUR GUIDE TO  
**FIGHTING  
FRAUD**

**PROTECT YOURSELF FROM SCAMMERS WITH THESE TIPS**



CHECK OUT  
**[Y12FCU.ORG/SECURITY](https://y12fcu.org/security)**  
FOR ADDITIONAL STRATEGIES  
ON FIGHTING FRAUD!

# Top Tips & Tricks

**+ When in doubt, reach out.**

Fraudsters impersonate merchants, financial institutions, and more. If you are unsure, end the communication to verify the source. Then, call us at 800-482-1043 to report an incident, and log in to your account to review your transactions and activity.

**+ Pause and think if you receive a weird link.**

Only click on links or open attachments if you know who sent them and what they are.

**+ Fraudsters are tricky, so be very picky.**

Never give personal or financial information to an unknown source. A fraudster may request payments by gift card, wire transfer, Venmo, Cash App, or another payment service.

**+ If account info's the wish, it's probably a phish.**

We will NEVER request sensitive information, including your Digital Banking passwords, security codes, and card information, such as the card number, PIN, or three-digit CVV code. We will also not call you and ask for any security or login codes texted to your phone.



**This includes the six-digit Y-12 FCU Digital Banking login code texted to your phone.**



**Pro Tip!**

Make sure you use strong online passwords and multifactor authentication when available.

# The ABCs of Fraud



## Clickbait

A story or link designed to attract a reader's attention and entice them to click on it.



## Malware

A malicious software that fraudsters use to damage or disrupt a computer to steal data or compromise networks.



## Phish / Phishing

A fraudster's method of impersonating an official entity or to trick the victim into giving out personal information.



## Skimmer

A device typically placed on or around a card reader to capture data from the card.



## Social Engineering

The use of manipulation by a fraudster to trick people into making mistakes or giving away sensitive information.



## Smish / Smishing

A fraudster's method of impersonating an official entity in the form of text messaging.



## Spoof / Spoofing

A fraudster's method of deliberately falsifying information of a caller ID display to disguise their identity and pretend to be another entity.



## Vish / Vishing

A fraudster's method of impersonating an official entity by making phone calls or leaving voice messages.

# Text Message Scams

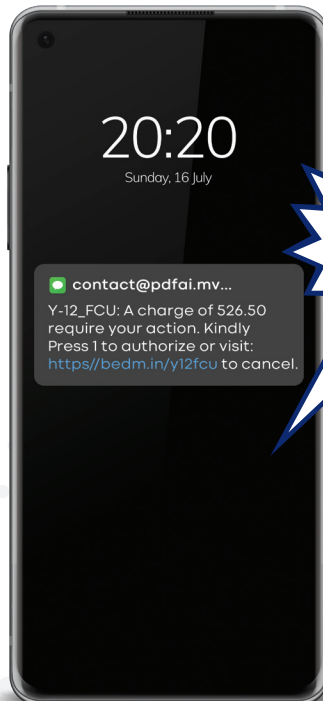
These **smishing** attempts impersonate a legitimate organization to social engineer you out of information or funds.

## Dos

- + Do slow down and think before you act.
- + Do keep your device and apps updated to the latest version.
- + Do delete the suspicious message to prevent accidentally replying.

## Don'ts

- + Don't click on any unknown links.
- + Don't send personal information.
- + Don't share authentication, access, and security codes.



# Email Scams

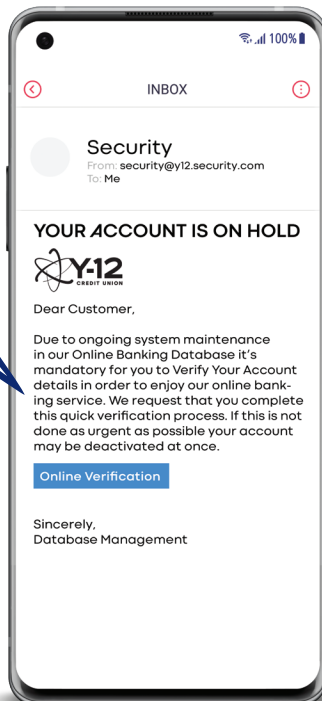
These **phishing** attempts impersonate an official institution to social engineer you out of information or funds.

## Dos

- + Do be skeptical of every email.
- + Do watch for attachments, typos, and grammatical errors.
- + Do delete the suspicious email to prevent accidentally replying.

## Don'ts

- + Don't reply, click on suspicious links, or download attachments.
- + Don't fall for urgency tactics or threats.
- + Don't send passwords or share personal information through email.



# Phone Call Scams

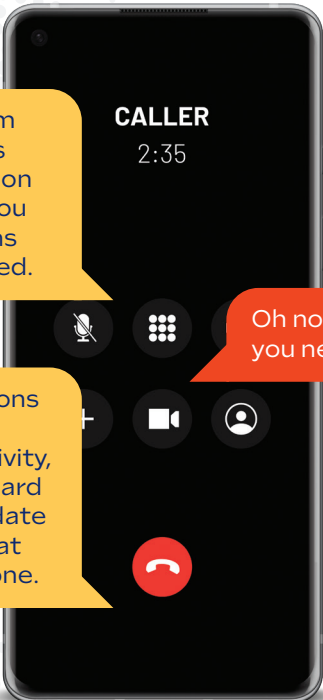
These **vishing** attempts impersonate a real entity to social engineer you out of information or funds.

## Dos

- + Do hang up even if it sounds legit.
- + Do verify the caller by finding the official number listed on the institution's website.
- + Do block the call and use call-blocking tools to screen unknown numbers.

## Don'ts

- + Don't rely on caller ID.
- + Don't fall for urgency tactics or threats.
- + Don't give personal or sensitive information over the phone.



Hi, this is John Smith from your credit union. There's some suspicious activity on your account and need you to answer a few questions so we can get this resolved.

We see several transactions that were flagged in our system. To verify the activity, please provide me your card number with expiration date and the six-digit code that was just sent to your phone.

Oh no! Absolutely. Whatever you need to get this resolved.

# Payment App Scams

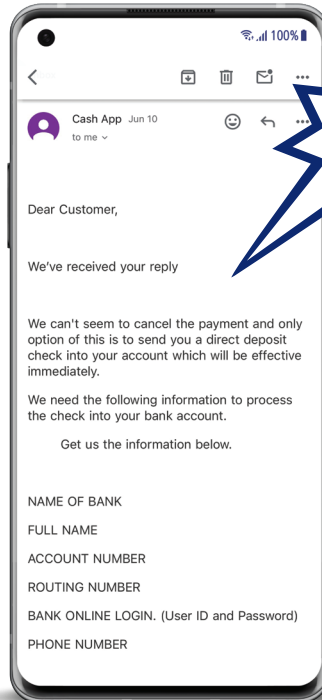
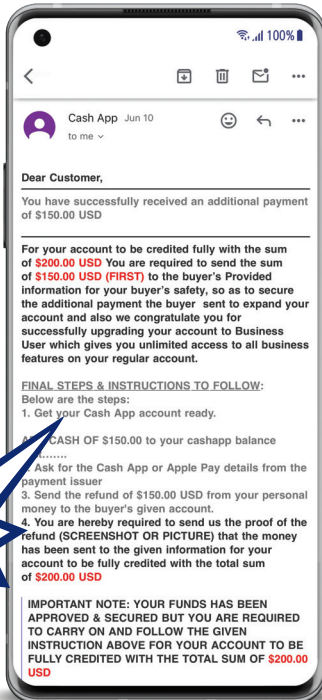
These **phishing** attempts impersonate a buyer or seller to social engineer you to get on one or multiple apps for money exchange.

## Dos

- + Do use payment apps to pay friends and family only.
- + Do use the Y-12 Credit Union app to monitor your account activity.
- + Do be wary of texts or calls about payment apps.

## Don'ts

- + Don't fall for urgent or unusual payment requests.
- + Don't send or accept payments from someone you don't know.
- + Don't send money in order to collect winnings for a prize.





# Social Engineering Techniques

## + Contest Scams

The fraudster reaches out to “contest winners” asking them to fill out forms with sensitive and payment information. They may require a cash payment to collect winnings.

## + Employment Scams

The fraudster requests training payments or sensitive information for a remote position.

## + Marketplace Scams

The fraudster presents as an average seller/buyer but tries to alter the exchange, such as changing the price, payment method, or communication platform.

## + Multiplatform Impersonation Scams

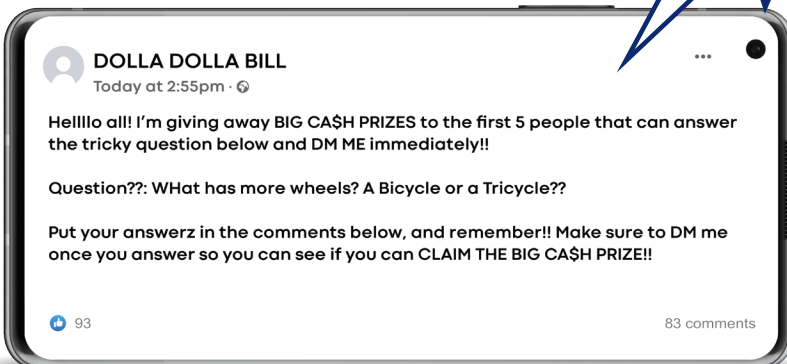
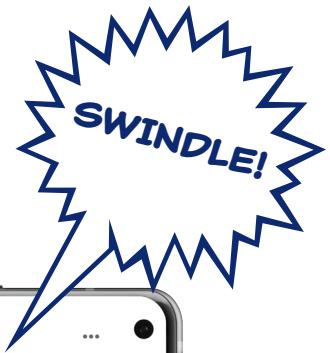
The fraudster starts communication on one platform like a marketplace app and impersonates official institutions through other platforms like email or text to request payments and sensitive information.

## + Romance Scams

The fraudster uses a fake persona and manipulation in the form of a love or friend interest to request money.



**Most Popular Scam**





# What to Do If You're a Victim

1

If you believe a scammer has your sensitive information like your Social Security number or bank account number, go to **IdentityTheft.gov** for next steps.

2

Monitor and potentially freeze your credit with the credit bureaus.

3

Freeze and report any compromised card.

4

Reach out to us at **800-482-1043** to report the scam.

5

If you lost money, file a police report.

6

Change any compromised username and password and implement multifactor authentication if your credentials were shared.

7

Report the scam to the Federal Trade Commission (**ReportFraud.ftc.gov** or call **877-FTC-HELP (877-382-4357)**) and to the Internet Crime Complaint Center (**ic3.gov**).

 You can cut out this page and keep it handy for future reference!



[y12fcu.org/security](https://y12fcu.org/security)