

Access Denied: Keep Hackers Out!

Phishing Scams

In phishing scams, criminals send emails, texts, or messages that appear to come from trusted organizations or contacts. These messages often claim there is a problem with an account or that immediate action is required. Victims are directed to click links or provide personal information such as passwords or account numbers. The goal is to steal login credentials or financial information.

RED FLAGS

- Messages creating urgency or fear, such as account suspension warnings.
- Links or attachments from unexpected or unfamiliar senders.
- Requests for personal or login information through email or text.

BE SCAM SMART

- Do not click links or open attachments from unsolicited messages.
- Verify messages by contacting the organization directly using a trusted source.



- Use strong, unique passwords and enable two-factor authentication.

Robocall Scams

Robocall scams use automated phone calls to deliver false warnings, offers, or requests. The caller may claim to be from a bank, government agency, or service provider. These calls often prompt you to press a number to resolve an urgent issue. The intent is to collect personal information or direct you to a scammer.

RED FLAGS

- Automated calls claiming urgent problems or legal threats.
- Requests to press a number or stay on the line to "fix" an issue.
- Caller ID information that appears suspicious or unfamiliar.

BE SCAM SMART

- Hang up immediately on unsolicited robocalls.
- Do not press buttons or provide information during automated calls.
- Register your phone number with the National Do Not Call Registry and use call-blocking tools.

CONTINUED



Identity Theft Scams

In identity theft scams, criminals steal personal information to open accounts, make purchases, or commit fraud in your name.

This information is often obtained through phishing, data breaches, or stolen documents. Victims may not realize the theft until they notice unfamiliar charges or account activity. The damage can be long-lasting and difficult to reverse.

RED FLAGS

- Unrecognized charges or accounts appearing in your name.
- Bills or collection notices for debts you do not owe.
- Alerts about account changes you did not make.

BE SCAM SMART

- Monitor bank statements and credit reports regularly.
- Shred sensitive documents and protect personal information.
- Report suspected identity theft immediately to financial institutions and authorities.

Where to Report a Suspected Scam

- FBI Internet Crime Complaint Center (IC3):
complaint.ic3.gov
- Identity theft report & recovery:
identitytheft.gov
- General fraud (FTC):
reportfraud.ftc.gov
- National Elder Fraud Hotline:
833-FRAUD-11 (833-372-8311)
- FL Office of Inspector General:
legacy.myfloridalegal.com/contact.nsf/contact?Open&Section=Citizen_Services
1-866-9-NO-SCAM
- U.S Department of Health and Human Services Office of Inspector General:
oig.hhs.gov/fraud/report-fraud
1-800-447-8477
- If your credit card or bank information has been stolen, contact your bank or credit card issuer directly.