How to spot SCAMS

- IT'S A - MONEY THING®

If you use a cellphone or have an email account, you've likely been exposed to an attempted scam



TYPES OF SCAMS

Familiarizing yourself with common scams can help you spot them before they turn into costly mistakes

UNEXPECTED MONEY

THE SETUP

A wealthy person asks the target for help with the transfer of a large sum of money, or an estate lawyer notifies the target of a large inheritance from a distant relative



THE SWINDLE

The target is required to pay fees, write a check or provide bank account access in order to complete the transfer of funds; the target never receives the money

UNEXPECTED WINNINGS

THE SETUP

The target is notified that they've won a lottery, a contest, a sweepstakes or some other prize giveaway



THE SWINDLE

In order to claim the (invented) prize, the target is instructed to pay a lottery tax or provide personal information

BUYER-SELLER FRAUD

THE SETUP

The target comes across a tempting online listing for a premium item at an extremely low price



THE SWINDLE

Scammers collect the payment but never deliver on the product; multiple accounts and fake reviews are used to disguise their deceptive practices

FAKE CHARITIES

THE SETUP

The target is contacted by a charitable organization and asked to make a donation



THE SWINDLE

Scammers pose as existing charities or invent fake ones and then pocket the donations

DATING SCHEMES

THE SETUP

The target is charmed by a new online sweetheart and develops an emotional bond with them



THE SWINDLE

The new sweetheart is actually a scammer; once the relationship has developed, the scammer asks for expensive gifts, travel or cash

GET-RICH-QUICK SCHEMES

THE SETUP

A job placement service offers to find a position for an unemployed target, or the target is approached by a businessperson with an investment opportunity



THE SWINDLE

The scammer collects placement fees for their fraudulent job placement service, or takes off with the target's investment money

THREATS AND EXTORTION

THE SETUP

The target receives urgent demands for money from a government official or from law enforcement, or the target discovers ransomware on their computer



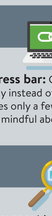
THE SWINDLE

The scammer poses as an authority figure to scare the target into paying them; the scammer holds computer files hostage to pressure the target into paying them

IDENTITY THEFT

THE SETUP

The target is asked to log into their account or confirm their password, or the target is contacted by a friend or relative and asked a series of questions



THE SWINDLE

The scammer impersonates the target's personal and business contacts in order to gain personal details that can then be resold or used for identity fraud

REPORTING SCAMS

If you believe you've been targeted by a scammer, contact the following:

INTERNET CRIME COMPLAINT CENTER (IC3)

www.ic3.gov

FEDERAL TRADE COMMISSION (FTC)

www.FTC.gov/complaint



Scams are often under-reported because of embarrassment or shame

STAYING SAFE

Buy some time: In an emergency, it's natural to act before you have time to think. It's no coincidence that many scams are designed to encourage an immediate reaction, before you have a chance to spot any red flags. Allow yourself to take a minute to assess a situation, even if it seems urgent.

Use the address bar: Get in the habit of visiting websites directly instead of following links contained in emails. It takes only a few extra seconds and helps you be more mindful about your online activity.

Cross-reference: It's perfectly reasonable to verify the identity of the person or business you're in contact with. Use a means outside of the original communication, like doing a separate web search or returning a call through a publicly listed number.

BROUGHT TO YOU BY

FIRST CREDIT UNION

Sources: FBI.gov, USA.gov, Australian Competition and Consumer Commission

- IT'S A - MONEY THING®

It's a Money Thing is a registered trademark of Currency Marketing