

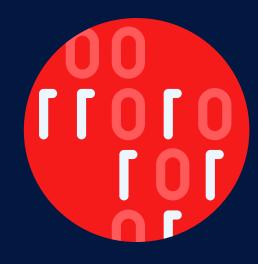
Impersonation Scams

The FTC Consumer Sentinel Network reported a sharp increase in Impersonation Scams. Here's what you need to know.

By the numbers

\$1.1 Billion

Total losses due to impersonation scams in 2023





5X increase

In reported consumer losses compared in 2020

Common types of impersonation scams



Tech support scam

The scammer claims to be an employee of a major corporation and has noticed a virus or issue with your computer.



IRS or tax scam

The scammer claims you owe back taxes and directs you to provide banking information to clear the charge.



Banking scam The scammers say there's an

issue with your banking information and to provide updated details to "fix it."



Fake giveaway The scammer lets you

know you've won a major prize—you just need to fill out information or pay a small fee to get it.



The scammer informs you of a problem with your

delivery problem

delivery and directs you to a fake website to steal your information.



The scammer pretends to be a government official and

agency scam

tells you to provide information, take specific action, or risk legal action.

of business impersonation in 2023

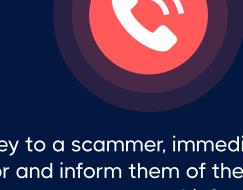
333,000 reports





of government impersonation in 2023

What if you fall victim to an impersonation scam?



If you've paid money to a scammer, immediately contact your bank or payment vendor and inform them of the fraudulent transfer. If a scammer has access to your personal information or accounts, change your passwords and major account details.

You should also report it to the FTC at ReportFraud.ftc.gov.



Anyone can fall victim to cybercrime. The right tools and

education keep you safe. Contact CertifID for help.

https://www.ftc.gov/news-events/data-visualizations/data-

spotlight/2024/04/impersonation-scams-not-what-they-used-be