CONNECTICUT CONSUMER PROTECTION MONTHLY NEWSLETTER

Volume 2 / Issue 9 / September 2025

SCAM ALERT

What it is: Wrong Number Text Scams

How it works: Scammers text you pretending they've reached the wrong number. Examples of messages might be:

- "Hey! Are we on for dinner tonight?"
- "Do you have a moment to talk?"
- "Hello?"

These wrong number texts are used to confirm your number is active, then they start with casual conversation to gain your trust and steal your personal or financial information.

How to protect yourself:

Do not respond or click any links in texts from someone you do not know. Be proactive by reporting or blocking the number.

Never share personal or financial information over text, especially if you have not verified their identity.

IMPERSONATION SCAMS: FACT OR FICTION?

Impersonation scams are on the rise again. In recent months, common imposter scams included text messages notifying you about an unpaid toll or missed jury duty.

Scammers are impersonating employees across several industries: government agencies, tech support, major retailers, and customer service teams. Consumers lost **$2.95 billion** to impersonation scams in 2024 in the United States, according to the Federal Trade Commission.

If you receive a message claiming to be from a business, government agency, or customer support team, ask yourself the ABCs:

ACTION: Are they demanding an immediate action? Is the caller asking for payment or to verify your account?

BUTTON: Is there a button, like a link to click, or a photo, or attachment to download?

CONSEQUENCE: Does the message threaten a consequence if the action is not completed? Will there be a hold placed on your account? (Jail time, fines, etc.)

If you answer **"YES"** to the above questions, it could be a scam. This type of scam is called "phishing" – the sender poses as a well-known figure or organization alerting the recipient of a fake problem and demanding urgent action. They will intimidate the recipient with a consequence if that action is not completed.

Scammers use scare tactics to convince recipients to send money, fill out personal information, or click a harmful link. **If you receive a message like this, report it as junk, block the sender and delete the message.**

Some additional red flags of imposter scams include:

- Pushy requests for personal information
- Email addresses end in "@gmail.com" "@yahoo.com" or a domain other than the company's name

SPEAKING REQUESTS

Want DCP to speak to your organization, or table at your event? Contact Catherine Blinder at Catherine.Blinder@ct.gov to submit a request.

Contact Us

Connecticut Department of Consumer Protection
450 Columbus Boulevard, Suite 901
Hartford, CT 06103-1840
Main Line: (860) 713-6100
(8:30 a.m. – 4:30 p.m.)

Consumer Complaint Center
(860) 713-6300
Toll Free: (800) 842-2649
8:30am-4:30pm
Email:
DCP.complaints@ct.gov

VISIT US ONLINE
CT.GOV/DCP

- Typos, grammatical mistakes, or awkward language
- Prompts to click a link or download attachments to "view more information"
- Caller claims to be "customer support" and asks for account password or suggests you make a new account over the phone

If you receive a suspicious message from a service you engage with regularly, **don't interact with it**. To confirm that the alleged issue is fake, contact the company directly.

Looking up "[company name] customer service number" in a search engine may direct you to a fraudulent phone number.

Instead, use the customer service number located on the company's website, app, mailing item, back of credit card, etc.

Transfer It to Protect It Money Scams

"Transfer It to Protect It" money scams are on the rise in the U.S.

Reported loss due to impersonation scams for adults 60 years or older:

2020 $55 million

2024 $445 million

A caller impersonating a bank, retailer, or government agency notifies you that there's suspicious activity on your account. and your finances are at risk. The caller may use phrases such as:

"Your ID is being used in criminal activity"

"Your computer has been hacked"

"Someone is using your account"

To protect your money, they urge you to transfer it into a "security account" via cryptocurrency (Apple Cash, Bitcoin ATMs)

In some reports, scammers claimed to be from the Federal Trade Commission (FTC) persuading people to hand over stacks of cash or gold to couriers.

If you receive a similar call, hang up and report the incident to ReportFraud.ftc.gov

Have a tip we missed? A topic you want more information about? Send us an email at DCP.Communications@ct.gov.