

CPF 00004-19-CID361-9H

27 March 2019



## Telephone Frauds and Scams

Every year, telephone scams and frauds affect millions of people. Although there are many variations of telephone frauds, there are a few basic kinds the Army family should be aware of. With a general awareness of telephone fraud, and a generous amount of caution, the likelihood of falling victim to these frauds can be reduced.

### Fat-Finger Frauds

Fat-finger is a colloquial term that, in this context, means simply misdialing a telephone number. Often, it is a misdialed toll-free area code. There was a time when the only [toll-free area code](#) was 800. But toll-free area codes can be 800, 888, 877, 866, 855, and 844. Scammers buy toll-free numbers that look like recognized and commonly called numbers but change the toll-free area code. [Vanity telephone numbers](#) are favorites.

For instance, while 888-3MY-BANK might be the correct number to reach *My Bank*, scammers can register 877-3MY-BANK, 866-3MY-BANK, 855-3MY-BANK, and so on. (Yes, it is legal.) If a *My Bank* customer misdials the toll-free area code he or she connects directly to a scammer. The scammer acts and sounds like the real *My Bank*. The bank's customer, believing they are connected to the real *My Bank*, reveals personal information.



### Telephone Support Scams

There are telephone support scams. Someone tells you they are from the computer support department of a computer manufacturer. Often, the caller will identify the brand of the computer being used and offer technical support for a fee. Or, offer free technical support if allowed to remotely connect to your computer. This is a scam. Do not provide any information to the caller or allow the caller to remotely access your computer. Legitimate technical support will not call you when there is a problem. They do not monitor the functioning of your computer.

### Shock and Awe

A scammer calls you, claims to be from a government entity, a court, the IRS or other government agency, an insurance company, a debt collection company, or some other similar entity. The caller forcefully and aggressively tells you are delinquent – a debt has gone past due and your credit score will be destroyed, or your taxes are unpaid and the police will soon be at your door to arrest you.

**Contact Information:**  
**Cyber Criminal Intelligence Program**  
**27130 Telegraph Road**  
**Quantico, Virginia 22134**

**Phone: 571.305.4482 IDSN 2401**  
**Fax: 571.305.4189 IDSN 2401**

**Email**

**CCIU Web Page**

**CID LOOK OUT**  
**ON POINT FOR THE ARMY**

**DISTRIBUTION:**

**This document is authorized for the  
widest release without restriction.**



**"DO WHAT HAS TO BE DONE"**

The caller tells you payment must be made immediately – in the form of gift cards, reloadable cash cards, or even cryptocurrency. It sounds odd. You do not think your taxes are delinquent or any debts are past due. But the caller is insistent and convincing and makes you feel as though you cannot ignore the problem.

This is a scam. Don't provide any information. Hang up. Remember, notices of past due debts or delinquencies will first arrive in U.S. mail.

Protect yourself from being the victim of a telephone fraud:

- Carefully dial telephone numbers.
- Be suspicious of any caller being forceful and demanding. Do your best to slow the conversation and not buy into threats.
- Be suspicious of any request to make payment by gift card, cash card, cryptocurrency or other odd form.
- Do not rely on the caller to give you a telephone number to call back. Verify any number by checking official statements or checking the company's or government agency's website.
- Do not provide credit card numbers, debit card numbers, bank account information or other personal information unless you have positively verified the authenticity of the caller.
- Remember, banks, utilities, lenders, government agencies do not threaten and notices of past due or delinquencies will arrive in U.S. mail.
- Do not be reluctant to hang up. If they call back, hang up again. Until you have verified the source of the call, keep hanging up.
- Hang up on prerecorded calls. Do not press 1 to talk to an operator. If possible, block the number from calling your phone.

## Resources

[Common Scams and Frauds](#) – USA.gov

[Fake Calls from Social Security](#) – Consumer Reports

[Fake Calls about Your Social Security Number](#) – Federal Trade Commission

[One Ring Phone Scam](#) – Federal Communications Commission

[Six Scams Service Members Should Watch Out For](#) – USAA

[Virtual Kidnapping Fraud](#) – CID

[Avoid Taxing Telephone Scams: Just Hang Up](#) – CID

To receive future CCIU Cybercrime Prevention Flyers, send an email to: [usarmy.cciuintel@mail.mil](mailto:usarmy.cciuintel@mail.mil) with "SUBSCRIBE: CPF" in the subject line.



**CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.**

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.