



Social Engineering and Account Takeover Schemes



Table of Contents

Social Engineering - What is It?

Trends and Statistics

Case Examples and Red Flags

What to do if you become a victim

Resources



Social Engineering - What is It?

Social Engineering is a scheme devised to obtain sensitive and/or private information about a person, such as a personal identification or bank account details, to access or obtain financial services.

In some instances, bad actors are after a person's computer and/or credentials to banking applications.

Trends and Statistics

Fraud is a growing problem. According to the FTC, reported consumer losses increased to \$12.5 billion in 2024, up 25% from 2023.

Phone calls continue to be the highest reported contact method by bad actors.


These statistics only represent what has been reported. In many cases, these incidents are not reported, either due to a minimal fraud loss, or the victim being embarrassed to admit they've been scammed.

Victims should always report fraud to the FTC ([FTC.gov](https://www.ftc.gov)). This way, new trends can be detected and shared with financial institutions and law enforcement, which will put them in a better position to mitigate and prevent further abuse.

What are the most common types of Social Engineering?

- Phishing
- Pretexting
- Spear-Phishing
- Baiting

If it sounds too good to be true, it probably is.

A hand holding a pen, writing on a notepad. The background is a light gray grid pattern.

Email Phishing

Phishing means exactly what it says - the sender is trying to get you to respond. In most cases, they will indicate they need an urgent answer.

Beware of links or attachments in emails, particularly if you don't know the sender and/or you didn't initiate the communication.

1) Email from domain (gmail) that doesn't match the company

dbmkufcjuydxv@gmail.com

Established companies do not use gmail accounts, and will have branded domains. Also, notice how this email was sent to 189 recipients.

2) Do you even have a Paypal account?

3) Urgent requests for you respond immediately or a negative consequence will result.

4) Never use a phone number in an unsolicited email. Search the company through their website to get a valid phone number.

1

Payment Successful Order 43232543546546

Pay Pal <dbmkufcjuydxv@gmail.com>

6/3/2025 3:01 PM

PP

To [redacted]@comcast.net and 188 others

Reply Forward Delete

1 attachment View Download

2



Customer Support Team: +1 (803) 745 3751

3

Dear PayPal Customer,

We have noticed an unauthorized transaction from your PayPal account. If this transaction was not made by you, please call us to cancel this order. Otherwise, your \$719.02 will be charged today.

Order Id: 277884144177239

Transaction Id: DTG326UWF758PQK

Apple iPhone 16

Colours: Ultramarine



Capacity: iPhone 16
256 GB

Description	Quantity	Specification	Amount
iPhone 16 256 GB	01	5G Mobile Phone with Camera Control, A18 Chip	\$ 719.02

Ensuring the security of your PayPal account is our highest priority, and we are committed to resolve the issues together in order to protect it.

Sincerely
Team PayPal

Customer Support Team: +1 (803) 745 3751

© 2025 PayPal All Rights Reserved

4

Unsolicited Text Messages

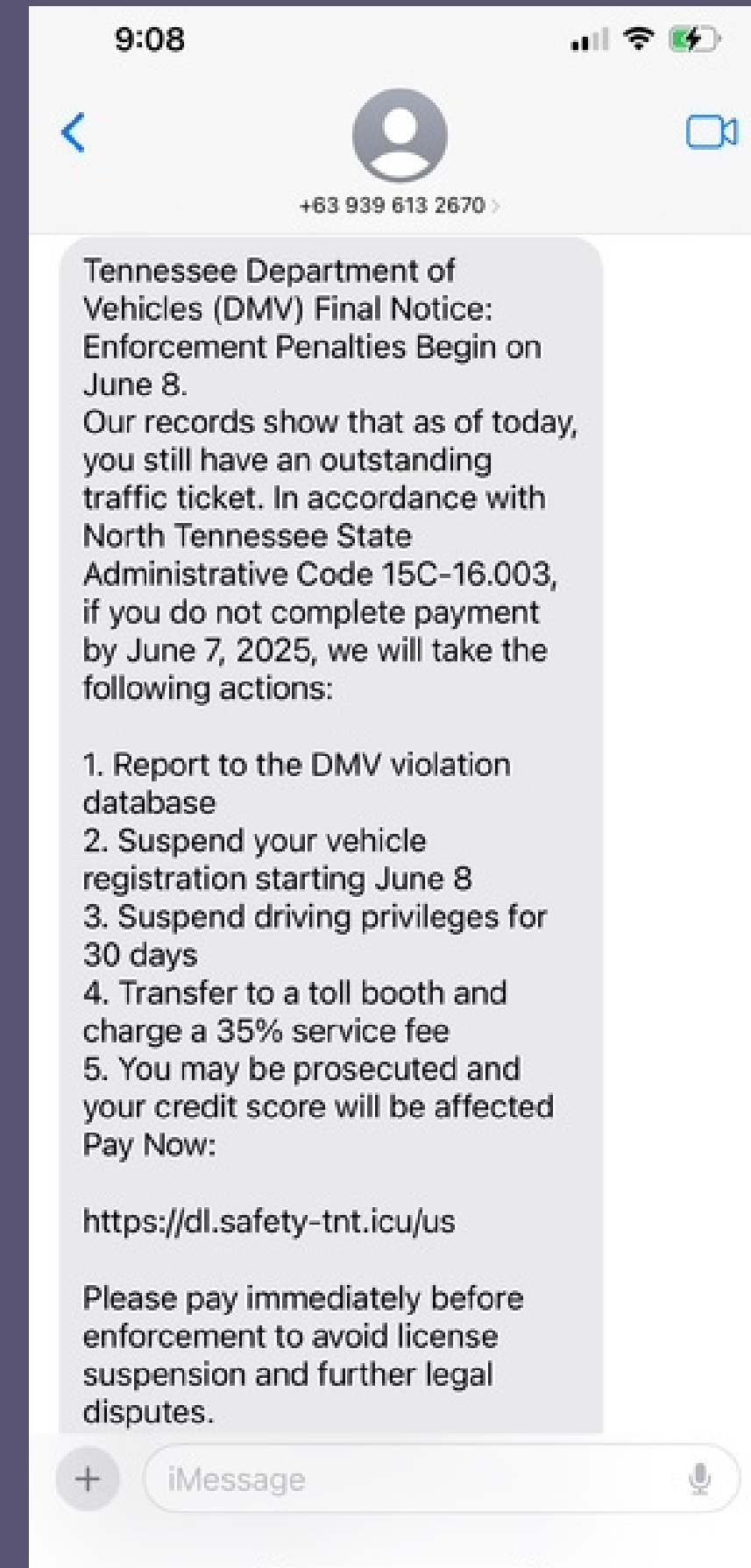
In this scenario, a text message is received that appears to come from a government/state authority, with a threat to revoke driving privileges.

Similar to the last example, payment is requested immediately, or there will be consequences.

In situations involving text messages, always check the sender's phone number (the number here is an international number, hence the "63" prefix. The state of Tennessee would not be sending messages out from this phone number.



Never respond to one of these texts,
even if you suspect it's a scam.
When you respond, the bad actor
knows they have hit upon a legitimate
phone number, and will continue
attempting to swindle you.



Pretexting

Pretexting is a social engineering tactic intended to deceive the target. Common characteristics of pretexting include:

- Often includes information already familiar to the victim, such a call or email from a senior employee of their company.
- As with regular phishing, requests are made with a sense of urgency.
- Will seek sensitive information, such as user ID's, passwords or bank account numbers.

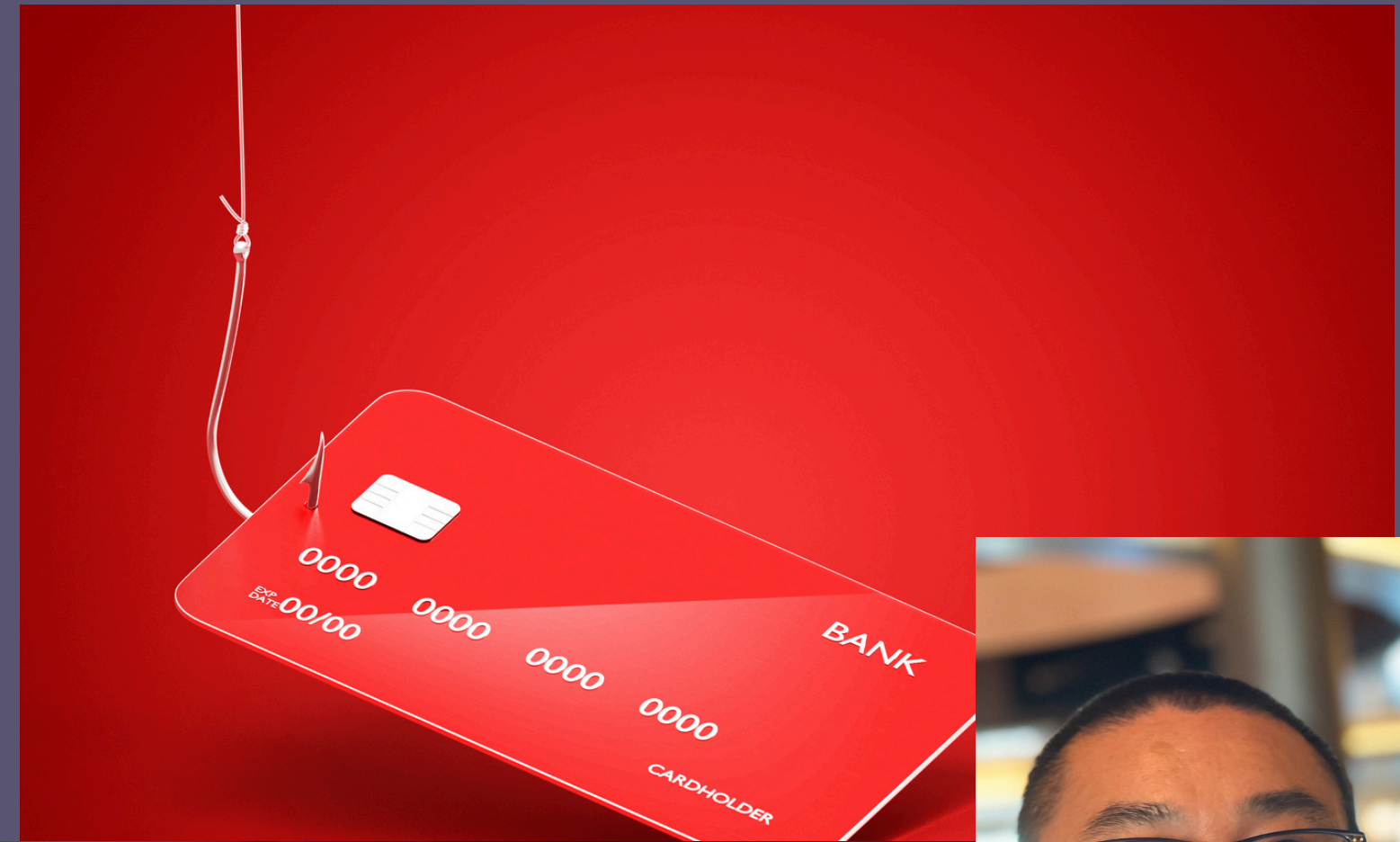


Baiting

Baiting works exactly as it sounds, and involves offering something of value or a “quid pro quo” with no intention of delivering.

The intent is to obtain information (usually bank account information), with promises of investment high returns, prize winnings or rewards.

In the scheme, the victim is often asked for a deposit, in order to “earn” their “reward”.



Don't Click or Respond!!

- Oftentimes, the solicitation will include a malicious link or attachment, that will install a virus or malware on your computer, subjecting your computer to takeover.
- If you respond (even if you know it's a scam), you have verified for the fraudster that your telephone number or email is a good, working contact. They will continue to contact you.
- Dependent on your level of participation in the scam, your bank may not reimburse you for fraud losses.
- Recovery on certain types of transactions (particularly wire and cryptocurrency) is extremely difficult, due to the speed of posting and ability to quickly move funds downstream from the target account.

What To Do If You Become a Victim

- Cease all communications with the fraudster
- Contact your bank and immediately place holds on any compromised accounts and/or bank cards
- Change passwords to any compromised accounts
- Immediately report the fraud to the Federal Trade Commission ([ReportFraud.FTC.gov](https://www.ftc.gov/report-fraud))
- Report the fraud to Internet Crime Complaint Center, IC3 ([IC3.gov](https://www.ic3.gov))
- Report the fraud to local police and/or Sheriff's office in your jurisdiction.
- Make sure your home computer and mobile devices have been restored with the latest virus protection software
- Contact your mobile phone provider to ensure your phone is clean and is no longer compromised.

What To Do If You Become a Victim

Other entities you may need to contact:

If your personal identification information (e.g., name, social security number and date of birth) has potentially been compromised, monitor your credit through [identitytheft.gov](https://www.identitytheft.gov).

Need Help?
**If you have questions or are a fraud victim
needing assistance, contact us.**



Email: support@fcvadvocacy.com

Phone: 888-264-2010

