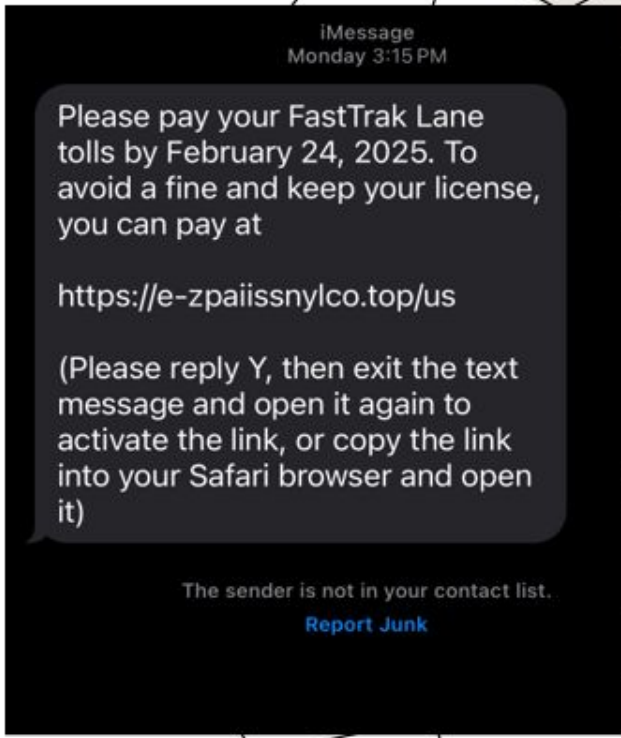
PHISHING SCAMS

Bruno Viera, Abraham Mustafa, Omar Alzubi,
Yasin Ahmed, Amid Qazi, and Jan Ulloa

WHAT ARE PHISHING SCAMS?

-A cyberthreat in which a scammer impersonates a trustworthy source

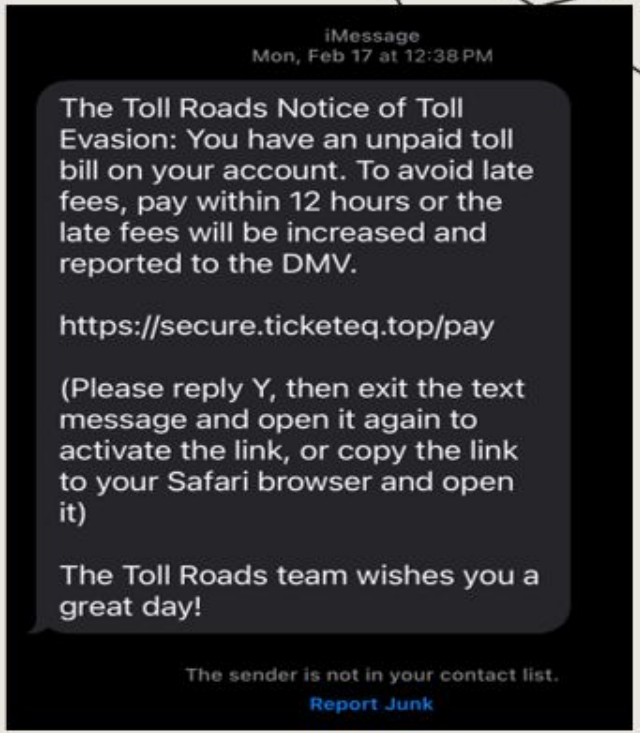
-Tricks individuals into revealing sensitive information such as passwords, bank account numbers, and Social Security numbers.



Look familiar?

The FBI's Internet Crime Complaint Center (IC3) reported receiving over 2,000 complaints about such phishing texts from early March 2024, indicating a widespread issue affecting multiple states.

In a controlled study conducted by Cornell University, out of 265 participants, 16.92% fell for simulated phishing attacks, with 12.82% succumbing to repeated attempts.



Internet Crime Complaint Center (IC3) | Smishing Scam Regarding Debt for Road Toll Services

[2212.13312] Users really do respond to smishing

IN CONNECTICUT

4.08 out of every 100,000 residents were victims of phishing scams in 2022

$26,093 was lost for every 100,000 residents to phishing scams in 2022

From Forbes: "Top Phishing Statistics By State"
Top Phishing Statistics By State – Forbes Advisor

CONNECTICUT PHISHING LAWS

Computer Crime (Connecticut General Statutes § 53a-251 to 256): Defines unauthorized access to computer systems, theft of computer services, interruption of computer services, misuse of computer system information, and destruction of computer equipment as criminal offenses.

Internet Crimes (Connecticut General Statutes § 53-451): Encompasses unauthorized use of a computer or computer network and unlawful sale or distribution of certain software.

Connecticut Law About Computer and Internet Crimes

TYPES OF PHISHING SCAMS

Spear phishing: Uses personal details (from social media or other public information) to craft convincing messages

Whaling: Targets high-profile employees via highly personalized, convincing messages to extract an organization's sensitive information.

Vishing: Phone calls or voice messages that pretend to be a reputable source.

Email Phishing: Mass emails sent by attackers posing as legitimate organizations.

EDUCATION AS A TOOL

About 36% of CT residents, or about 1.3 million people, lack the skills to meet the Digital Literacy Benchmark*

People should be taught that these scams are a business and to look out for common red flags:

- Suspicious email addresses or domain names
- Urgent or threatening language
- Unexpected attachments or links

*Annual Report of the Connecticut Commission for Educational Technology (2023)

SPREADING THE WORD

Social media platforms can be used to prevent people from becoming victims of phishing scams

Verified State Government accounts can post whenever a new scam emerges, showing an example and advising people to avoid communicating back with the sender or going to any links

AI POWERED DATABASE SOLUTION

Can submit messages (text, email, voicemail transcript) to a database, which is then analyzed by a trained AI model and given a percentage likelihood to be a phishing.

AI Model trained to detect phishing red flags

Constant access to a continuously updated source of potential threats and can track activity nearby

Can be expanded to detect and monitor any other kind of message-based scam as well

DATABASE USER FLOW

1. You receive a message you are suspicious of

2. Enter the database's website, where you can see current threats in your area.

3. If you don't already recognize your message as a threat, you can upload a copy of the message to the database

4. Trained AI model analyzes the message and returns a percentage likelihood of the message being a scam

5. Model creates a generic example using messages and uploads them to the website along with the scam likelihood percentage so others in the area have access to trending threats

USEFUL RESOURCES

- Phishing | Federal Trade Commission - Information from the FTC on how to recognize a phishing scam and what to do about it.

- ReportFraud.ftc.gov - Report fraud to the FTC

- Forward suspicious emails to the FTC at spam@uce.gov and to the Anti-Phishing Working Group at reportphishing@apwg.org