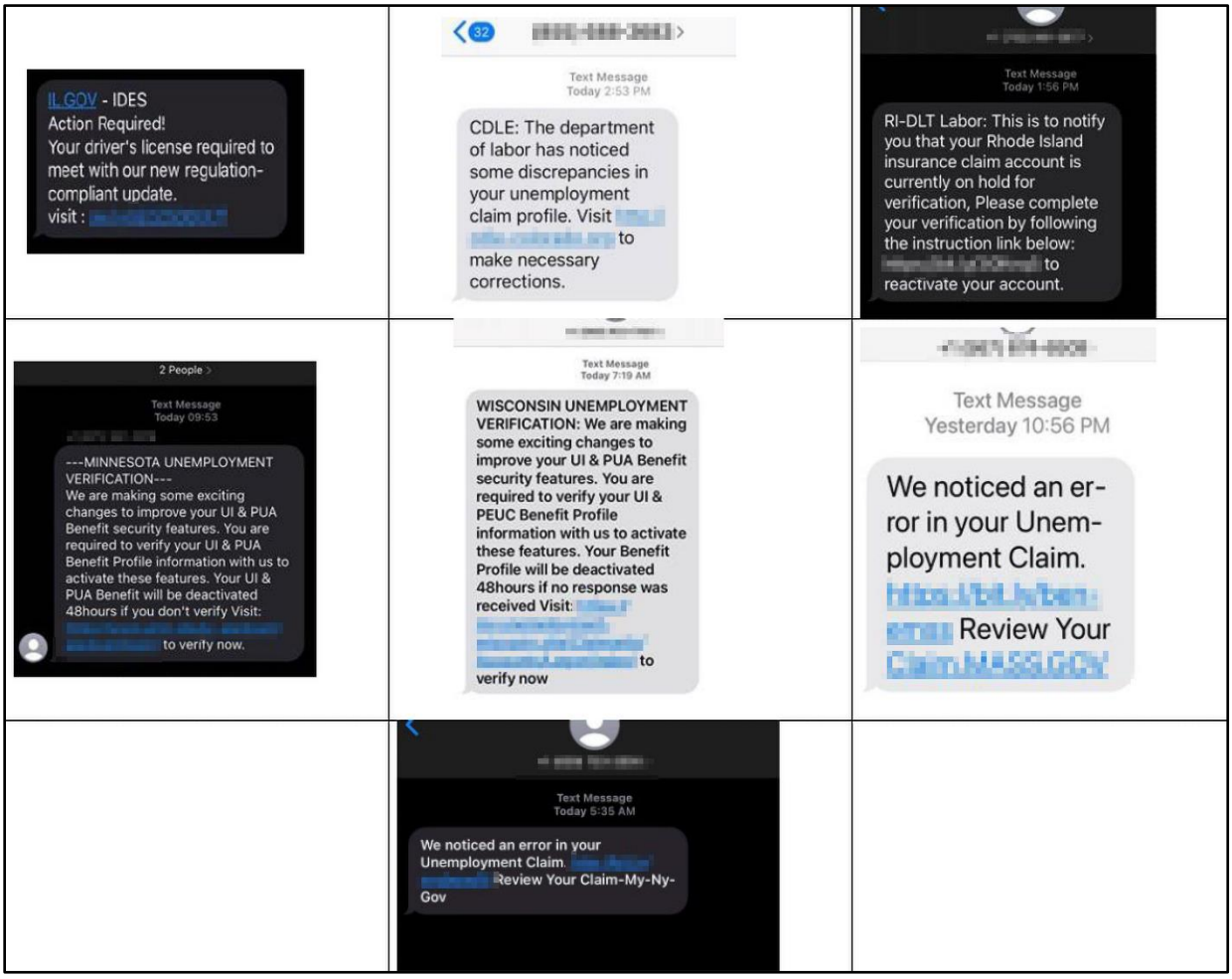
Phishing scheme targets unemployment insurance benefits and PII
August 4, 2021
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

Have you gotten an alarming text message about your unemployment insurance benefits from what seems to be your state workforce agency? You're not alone. Identity thieves are targeting millions of people nationwide with scam phishing texts aimed at stealing personal information, unemployment benefits, or both.

The phishing texts try to dupe you to click a link to "make necessary corrections" to your unemployment insurance (UI) claim, "verify" your personal information, or "reactivate" your UI benefits account. The link takes you to a fake state workforce agency (SWA) website that may look very real. There, you're asked to input your website credentials and personal information, like your Social Security number. Fraudsters can use the information to file fraudulent UI benefits claims or for other identity theft.

Here are examples of some of the phishing texts.



Protect yourself. Know that state agencies do not send text messages asking for personal information. If you get an unsolicited text or email message that looks like it's from an SWA, don't reply or click any link. If you're not sure, contact the SWA directly using the State Directory for Reporting Unemployment Identity Theft at the bottom of this United States Department of Labor webpage.

If you think you may have entered your personal information into a fraudulent website, visit IdentityTheft.gov to find out how to make it harder for an identity thief to misuse your information.

You can report a suspicious text message or email claiming to be from an SWA to the National Center for Disaster Fraud (NCDF) by completing an NCDF Complaint Form or by calling (866) 720-5721. Tell us too at ReportFraud.ftc.gov. And, tell a friend. By sharing your experience and knowledge about the fraud, you can help someone else avoid the trap.