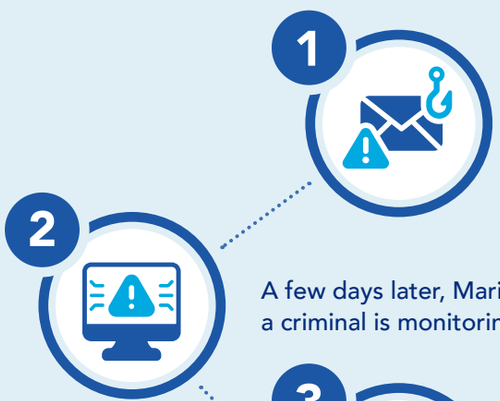
ACCOUNT TAKEOVER FRAUD SCENARIO: MALWARE

Scenario Overview

Maria unknowingly downloads malware after clicking on a link in an email about a missed delivery. Using the malware, the criminal monitors her keystrokes and steals her financial institution account credentials. This leads to an account takeover fraud incident in which $25,000 is stolen from her account.

Let's take a more detailed look at what happened in this scenario:



1. Maria receives an email about a missed package delivery. The email appears to be legitimate and contains her name. It asks her to open a link to "view delivery details."

   Maria clicks the link and unknowingly installs malware on her laptop.

2. A few days later, Maria logs in to her online banking. She is unaware that a criminal is monitoring her keystrokes with the malware.

3. The criminal attempts to log in to Maria's account. Because a new device is detected, a one-time passcode (OTP) is sent to Maria.

4. A new pop-up appears on her laptop screen that appears to be from her financial institution: "Your device verification is expiring and needs to be extended. Please enter the code sent to you to verify."

   Not thinking that there is anything unusual about this request, she enters the OTP as prompted.

5. The criminal sees the OTP that Maria entered and uses it to access her account. The criminal immediately disables security alerts on the account.

6. The criminal transfers $25,000 out of Maria's account.

7. A week later, Maria notices $25,000 is missing from her account. She contacts her financial institution to investigate.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.