Lookout Phishing AI Discovers Mobile-Only Banking Campaign

Advanced phishing attack imitates consumer banking login portals

Background and Discovery Timeline

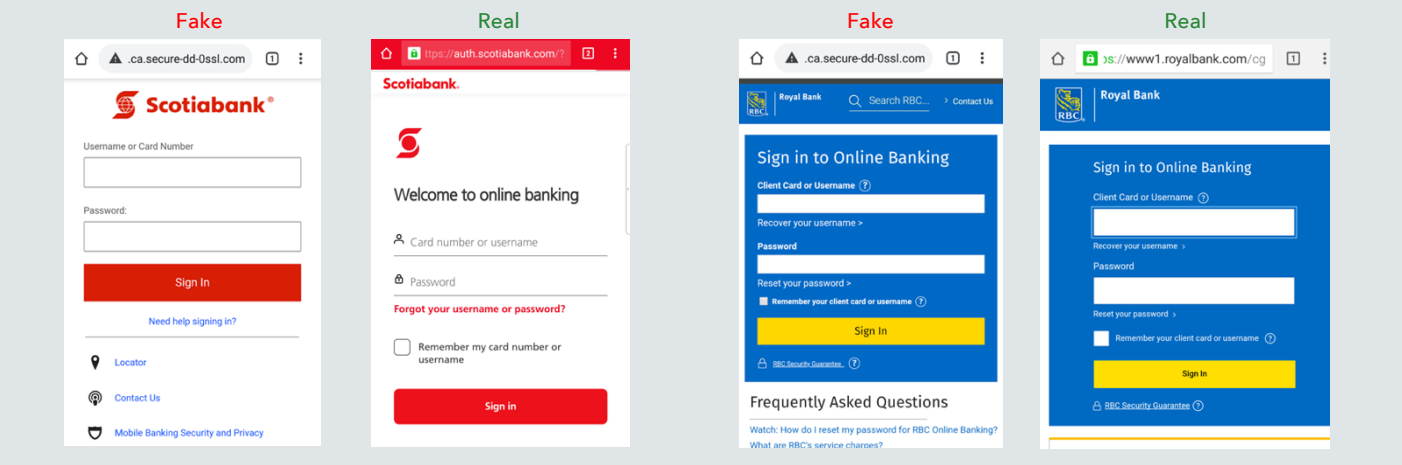
In early 2020, Lookout Phishing AI discovered a malicious phishing campaign targeting North American banking and financial institutions with a particular focus on customers of Canadian-based organizations. The campaign clearly targets mobile users, as it spreads via SMS messages and leads users to fake login pages built for mobile browsers. The back end of the campaign shows that the attacker built a tool to easily blast an SMS message to as many phone numbers as they want, which further indicates a mobile-first attack strategy.

Key Facts

1. This is a mobile-only phishing campaign.
2. Works by guiding bank customers through false account validation.
3. All institutions with potentially affected customers were notified upon discovery.

Capabilities and Affected Parties

Lookout researchers dove deeply into this campaign and were able to access the front-end platform that the attackers used to blast SMS messages to potential victims. These messages contain links to fake login pages that appear legitimate. If the victim is tricked, the attacker steals banking credentials by guiding the victims through a number of security questions such as verifying their account number or asking for their card's expiration date. With that information, they can easily surpass security questions and steal from the victim's account.



Lookout Phishing AI

With our advanced Phishing and Content Protection technology, Lookout is able to identify early signs of a phishing attack and build protection for Lookout users, as well as provide early warnings to Lookout partners before their customers are impacted.

Learn more about Phishing and Content Protection