



How the Gmail Scam Works



1  An attacker obtains a victim's email address and phone number—both of which are usually publicly available.

2  The attacker poses as the victim and requests a password reset from Google.

4 

The attacker then texts the victim with a message similar to:

"Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity."

6 

The attacker resets the password—and once he has what he wants or has set up forwarding— informs the victim (posing as Google) of the new temporary password, leaving the victim none the wiser.

3 

Google sends the code to the victim.

5 

The victim therefore expects the password-reset verification code that Google sends out and passes it on to the attacker.

