

How your email & Facebook can be hacked

Below is a video by Symantec, the company who created the Norton anti-virus software

https://youtu.be/dj_90TnVbo

Part 1 - Email

In the below example we will imagine that an attacker is attempting to hack into a Gmail account belonging to a victim called Alice.


Alice registers her mobile phone number with Gmail so that if she ever forgets her password Google will send her an SMS text message containing a rescue verification code so she can access her account.


Don't get locked out of your account!

Without recovery options, you could **lose all access to your account** if you forget your password or if your account is stolen. [Learn why recovery options are so important](#)



Add a phone number and a recovery email address to ensure that you can always regain access.

 **Phone number** (recommended)

 **Recovery email address**

Google will only use this information for security purposes. We won't share it with other companies without your explicit consent.

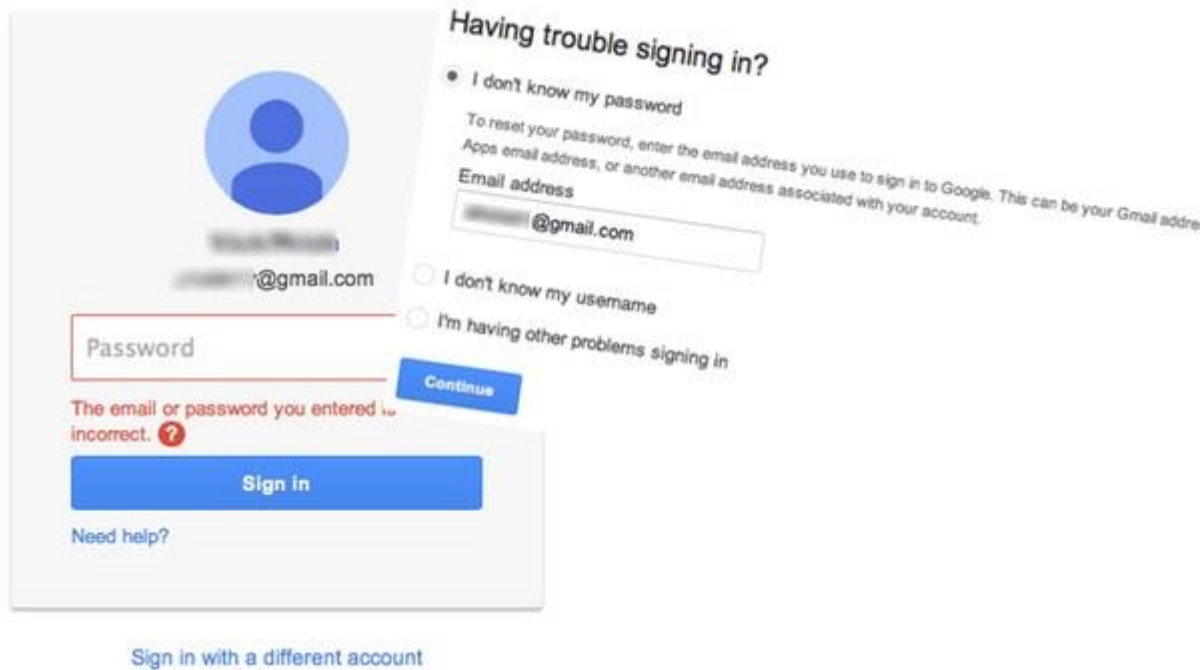
Done

No thanks

A bad guy - let's call him Malcolm - is keen to break into Alice's account, but doesn't know her password. However, he does know Alice's email address and phone number.

So, he visits the Gmail login page and enters Alice's email address. But Malcolm cannot correctly enter Alice's password of course (because he doesn't know it).

So instead he clicks on the "Need help?" link, normally used by legitimate users who have forgotten their passwords.

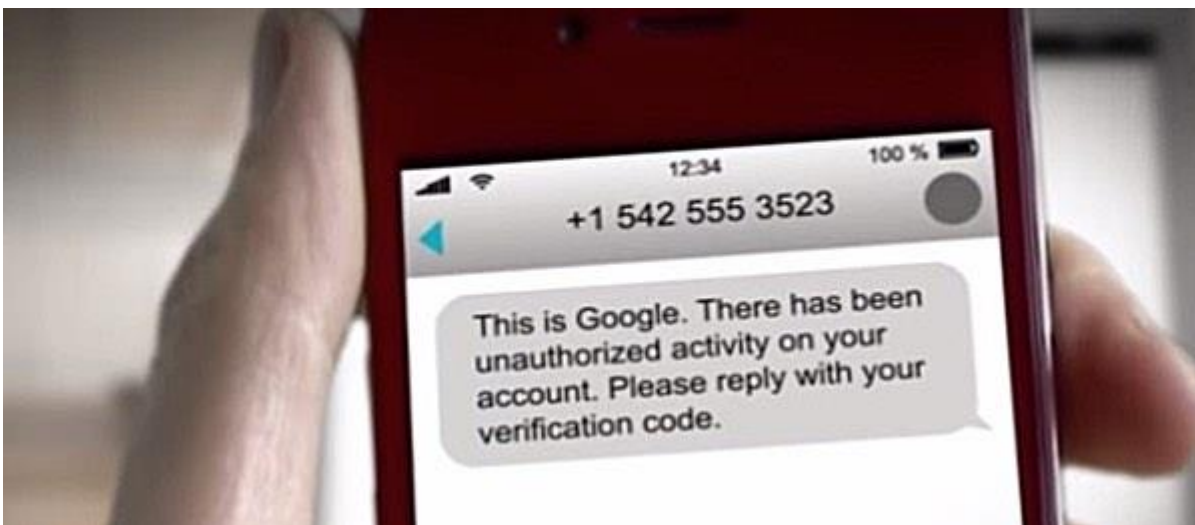


Rather than choosing one of the other options, Malcolm selects "Get a verification code on my phone: [mobile phone number]" to have an SMS message containing a six digit security code sent to Alice's mobile phone.

This where things get sneaky.

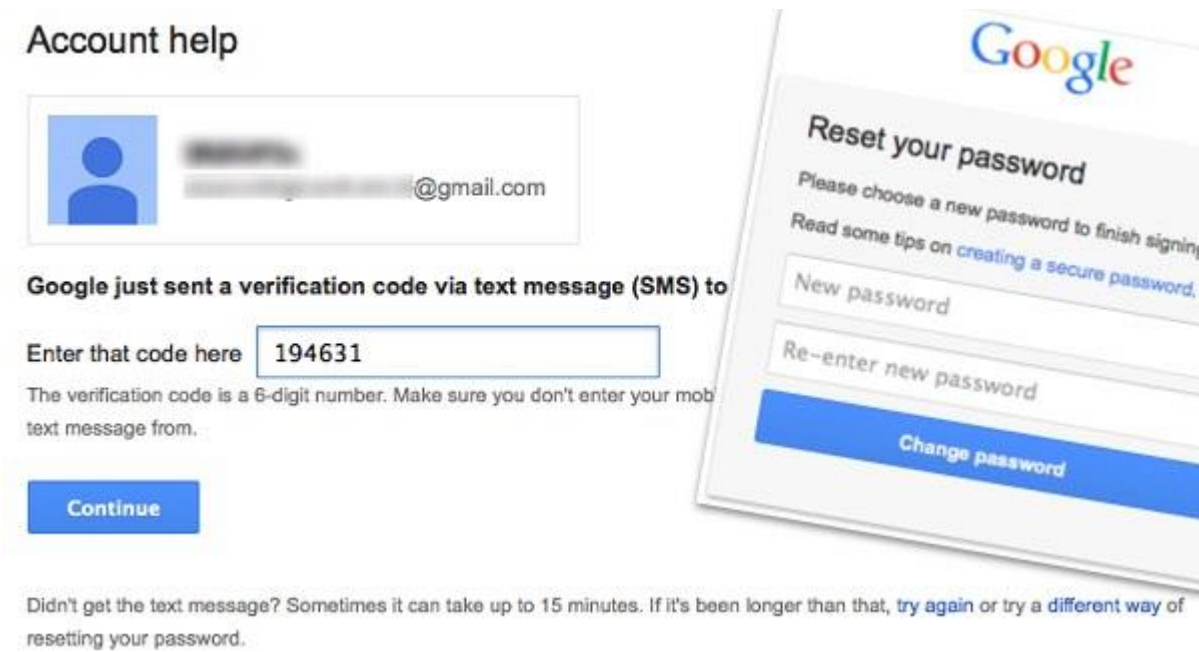
Because at this point, Malcolm sends Alice a text *pretending to be Google*, and saying something like:

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




Alice, believing that the message to be legitimate, replies with the verification code she has just been sent by Google.

Malcolm can then use the code to set a temporary password and gain control over Alice's email account.



Account help

 [Redacted] @gmail.com

Google just sent a verification code via text message (SMS) to

Enter that code here

The verification code is a 6-digit number. Make sure you don't enter your mobile text message from.

[Continue](#)

Didn't get the text message? Sometimes it can take up to 15 minutes. If it's been longer than that, [try again](#) or try a [different way](#) of resetting your password.

Reset your password

Please choose a new password to finish signing in.
Read some tips on [creating a secure password](#).

[Change password](#)

If Malcolm was keen to not raise suspicion, and continue to see every email that Alice receives for the foreseeable future, then it may be that he will reconfigure her email to automatically forward future messages to an account under his control, and then send an SMS to her containing the newly reset password:

"Thank you for verifying your Google account. Your temporary password is [TEMPORARY PASSWORD]"

Even if Alice changes her password at a later date, Malcolm will continue to receive her private email correspondence unless she looks carefully at her account's settings.

In short - it's a nasty piece of social engineering which it's easy to imagine working against many people.

So, what's the solution?

Well, the simplest advice is to be suspicious of SMS messages that ask you to text back a verification code - in particular if you did not request a verification code in the first place.

However, I wonder how many people when faced with a message that they believe to be from Google or Yahoo would act upon it immediately, with little thinking of the consequences. After all, one of the biggest worries many people might have in this day and age is to be cut off from their email account.

How any Facebook Account can be hacked

Part 2 - Facebook

The attacker first needs to click on the "Forgot account?" link on the Facebook.com homepage. Now, when asked for a phone number or email address linked to the target account, the hacker needs to provide the legitimate phone number.

The attacker then diverts the SMS containing a one-time passcode (OTP) to their own computer or phone, and can login to the target's Facebook account.

The issue affects all Facebook users who have registered a phone number with Facebook and have authorized Facebook Texts.

Besides Facebook, researchers' work shows that any service, including Gmail and Twitter, that uses SMS to verify its user accounts has left open doors for hackers to target its customers.

Although the network operators are unable to patch the hole sometime soon, there is little the smartphone users can do.

- Do not link your phone number to social media sites, rather rely solely on emails to recover your Facebook or other social media accounts.
- Use two-factor authentication that does not use SMS texts for receiving codes.
- Use communication apps that offer "end-to-end encryption" to encrypt your data before it leaves your smartphone over your phone's standard calling feature.

Update: However, the important thing to note is that the issue has actually nothing to do with Facebook security or other website's security, instead it is the weakness in the telecom network.

"Because this technique [SSL exploitation] requires significant technical and financial investment, it is a very low risk for most people," Facebook spokesperson told The Hacker News.

"As an added precaution, we recommend turning on two-factor authentication, called Login Approvals, in your Facebook security settings. Doing this will disable recovery via SMS on your account so even if someone has your phone number, they'll still need your password to access your account."