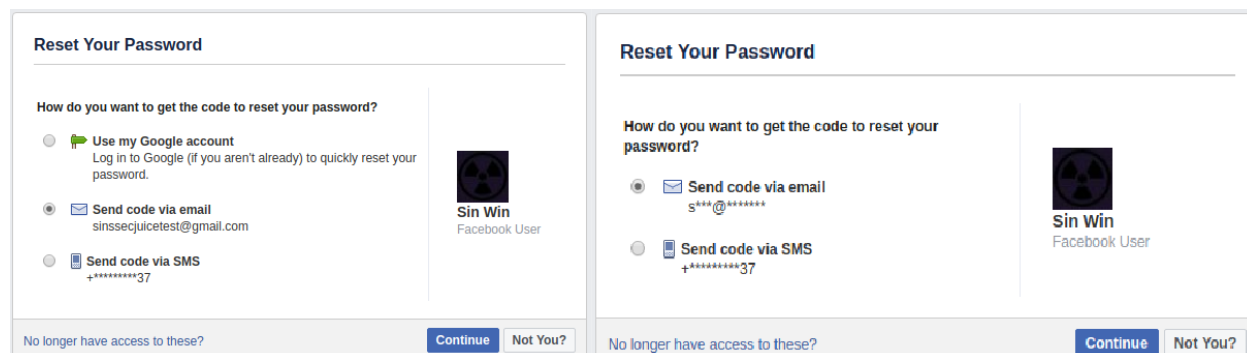


Account Knocking For Fun and OSINT

If you have been around on the internet long enough, chances are you've forgotten your account login to a website once or twice. Many platforms employ an Account Recovery technique which is designed to help users who do not remember their login information. This method can also be exploited by an investigator to gather information on a target. While this can be used on dozens of websites to differing effects, the following websites are ones that offer some of the best information on a target when you have only a snippet of information (email or phone number) to start off with.

Facebook



The image displays two side-by-side screenshots of the Facebook 'Reset Your Password' page. Both pages show the same options for how to receive a reset code: 'Use my Google account', 'Send code via email', and 'Send code via SMS'. The left screenshot shows the 'Send code via email' option selected, with the email address 'sinssejuicetest@gmail.com' visible. The right screenshot shows the 'Send code via email' option selected, with the email address 's***@*****' visible. Both screenshots show a profile picture placeholder and the name 'Sin Win' with the text 'Facebook User' below it. At the bottom of each screenshot are links for 'Continue' and 'Not You?'.

Facebook is the holy grail when it comes to gathering identifiable information on a target. Exploiting the account recovery technique on Facebook can be done with a target's email address or phone number. In order to exploit a target's Facebook, navigate over to the Facebook Account Recovery page [here](#). Enter the target's email or phone number and click search. The next page will display the results of the account connected to the search criteria. If you search via a phone number it will return an associated email with only the first character visible.

Be aware that the number of asterisks shown in the email is NOT consistent with the number of characters in the actual unredacted email. Searching via an email address will return a partially redacted phone number associated with the account that provides the last two digits. Both criteria will return a profile photo and the name associated with the account. You can take this information and do a search on Facebook for the target's name as provided by this technique and look for a matching profile photo to find the target's actual profile.

Keep in mind that while searching for a user on Facebook via their email or phone number requires the user to have it set to allowed. However, utilizing the account recovery technique will return the account's phone number and email regardless of whether they have it hidden or not.

Twitter

How do you want to reset your password?

We found the following information associated with your account.

- ☒ Text a code to my phone ending in **37**
- ☐ Email a link to **si*****@g****.*****

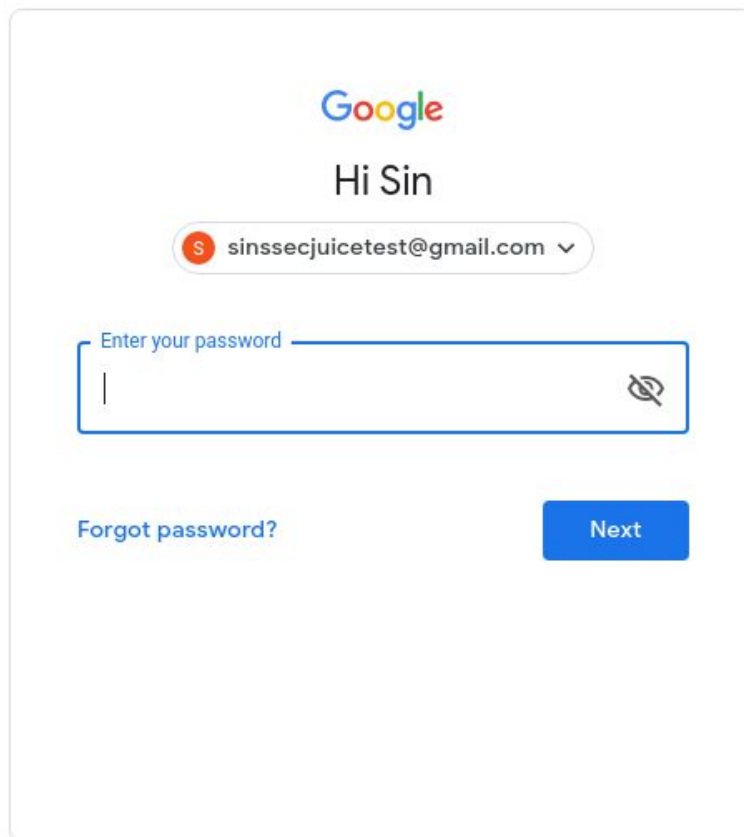
Continue

[I don't have access to any of these](#)

If your target doesn't have a Facebook account then the next step would be to look for a Twitter account. Head over to Twitter's account recovery page [here](#) and enter the target's email or phone number then click search. This search can also be done using the target's Twitter username as well. Unlike Facebook, the results from Twitter appear to be consistent regardless of whether you enter a target's email or phone number.

If there are any matching accounts Twitter will display the last two digits of the phone number connected to the account as well as a partially redacted email address. Unlike Facebook, Twitter's redacted email result will contain the same amount of characters as the actual email address on file. The first character of the email domain will also help narrow down the email provider. Keep this in mind when looking for potential matches on other platforms.

Gmail



The image shows a screenshot of the Gmail login interface. At the top is the Google logo. Below it is a greeting 'Hi Sin'. Underneath the greeting is a rounded rectangle containing a red circle with a white 'S' and the email address 'sinsecjuicetest@gmail.com' followed by a dropdown arrow. Below this is a password input field with the placeholder text 'Enter your password'. To the right of the input field is an eye icon. At the bottom left is a link 'Forgot password?' and at the bottom right is a blue button labeled 'Next'.


If your target has a Google email address you can extract their first name using Gmail's account recovery feature. Rather than utilizing the Gmail account recovery page, which requires additional verification, we will be using the Google login page found [here](#). Simply enter the target's Gmail address and click next. If you do not know the target's Gmail address, but know that they use the same username across multiple platforms, it might be a good idea to try that username as well and see if any matches appear. If the user has entered a name for their Gmail account the next page will display the user's first name with the greeting. Although the first name of a target might not be as valuable as a phone number or email address, it does assist in completing the overall picture of a target and might help narrow down possible suspects.


Yahoo


sinssecjuicetest

Recover your account

Select a verification method



 **Text (4**) ***-**-37** >
Msg & data rates apply

 **Email s*****st@gmail.com** >

[I need further help](#)

Employing the account recovery technique on a Yahoo email can help narrow down a target's information. Open up the Yahoo login page [here](#), and click on "the trouble logging in" link. Enter your target's Yahoo email address and click continue. The next page will return the account's associated telephone number and email address, both partially redacted. Unlike the previous platforms, Yahoo will also provide the first digit of the target's area code in addition to the last two digits. Likewise, the email address will return the first digit and the last two digits of the email address as well as the full email domain. These extra characters help build the overall picture of the target's contact information. Keep in mind however that Yahoo's partially redacted email does not accurately reflect the number of characters associated with the actual email address on file.

Apple

Apple ID

Confirm your phone number.

Enter the phone number that you use with your Apple ID.

(...) ---...37

Cancel

Continue

For targets that have an iCloud email, Apple's ID recovery page can be used to obtain partial information on an account's associated phone number. Just head over to the account recovery page [here](#) and enter the target's iCloud email address and click the Continue button. The next page will display a partially redacted telephone number providing the last two digits of the number that is on file for the account. Although not entirely useful on its own, gathering a target's telephone information via Apple has proved beneficial when the target did not otherwise link their telephone number on social media accounts that were previously exploited.

Conclusion

Although this investigative technique works on many other websites, the above platforms are the top five that have most consistently provided actionable intelligence on a target. Keep in mind that some websites will indeed send the target a verification email or text. If this occurs your target will likely be aware that something is going on and/or that someone is attempting to access their account. This may cause them to move to another email or social media account for future activity. For that reason, if you decide to attempt this technique on a platform other than those shown above I highly suggest you do as I did and create some temporary sock puppets to test on prior to using it on a live target.