Account Safety Guide

Tips to Keep your Account Safe

INTRODUCTION:

Greetings! We are super excited to have you on board as a member of the Kohaú executive team, and we hope you can make lasting memories here. With all the great people you meet here, you're going to meet some bad ones too. To put it simply, this document is a guide on how to not get hacked. If you follow everything in this guide and keep yourself aware of the common scams, your account will remain safe.

BASIC ACCOUNT SAFETY:

We expect all members of our team to have a basic understanding of internet safety. We hope the following points are common sense and extremely obvious to most.

- **Don't share your passwords to anyone online**.
- **Use a different password for every account**, especially your Roblox and Discord accounts. If you use the same password for everything, someone can hack your Roblox, login to your linked email with the same password, then completely lock you out of your Roblox account.
- **Don't share personal informatio**n such as your full name, address, face pictures, etc, to strangers online. This makes it easier for people to guess your passwords or hold you at ransom.
- **Set up 2-Factor Authentication** on your Roblox and Discord accounts, and **don't turn it off**.

The easiest but most important way to keep your account safe is by setting up 2-Factor Authentication (2FA). This doesn't make you immune to account theft, but it makes hackers' jobs a lot harder. It is important that you set up 2FA with an Authenticator App (such as Google Authenticator or Authy) and NOT simply with an email or phone number, as it's easy for hackers to spoof these and get access to your 2FA codes. Securing your Roblox, Discord and Email accounts with an

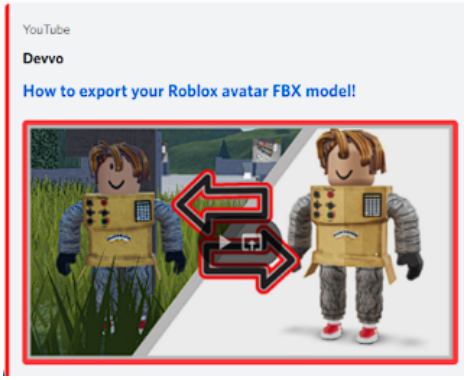
Authenticator App is the best way to protect your accounts, but this in itself won't prevent you from getting hacked.

SCAM AWARENESS:

Even with the most secure passwords and 2FA on your accounts, you'll likely still find people who are trying to steal your account. If you stay aware of the common account theft scams, you'll be less vulnerable to these types of attacks. Read below for an extensive list of almost all the types of scams you can be targeted by.

HAR/GFX Scam:

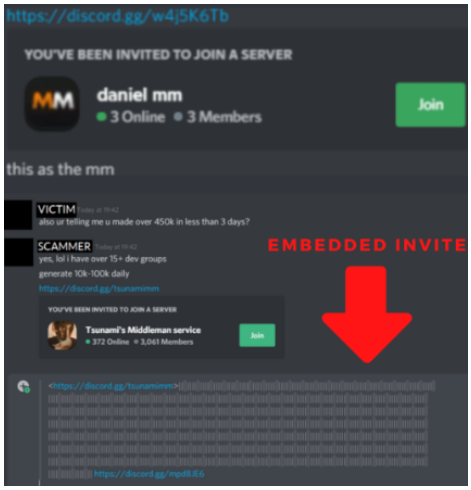
This method involves the scammer DMing a victim asking if they can make a GFX out of their avatar. They ask for your "avatar file" and send you a video tutorial on how to get this. In reality, if you send this file to someone, you give the scammer access to your account as the file contains your .ROBLOXSECURITY cookie.



Middle Man Scam:

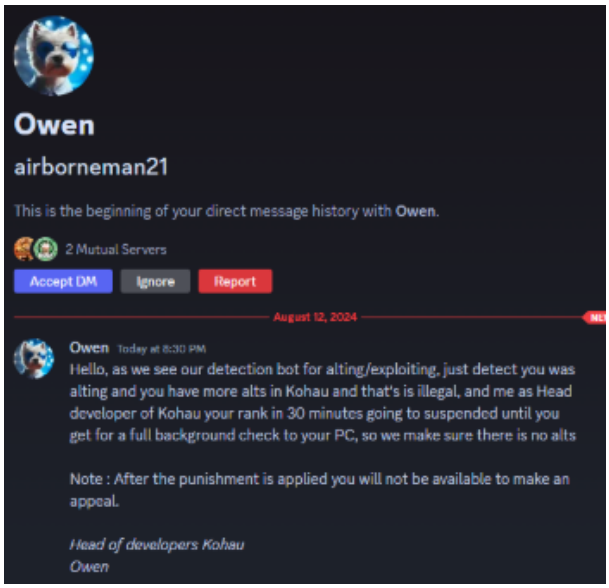
This method targets users with expensive Limiteds and can come in many ways. To avoid this scam, double check all users that could be impersonating others. Also check Discord invites and ask around for help if you're skeptical. Here are some examples:

- The scammer sends you a fake middle-man server (sometimes it's embedded)
- The scammer may pretend to be a trusted and known middle-man
- The scammer may put you in a group chat with a real middle-man then swap them out for a fake one and make you send your items to their alt



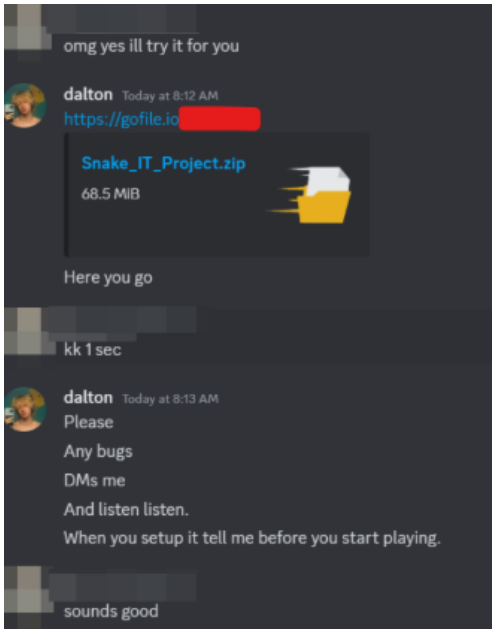
Screenshare Scam:

Usually this type of scam involves a user faking evidence of you doing something bad in order to get you banned from a server. After you are banned, they impersonate a staff member of that server and ask you to confirm account ownership by screen-sharing your password reset link (or other forms of personal information). In Kohaú, this scam is often in the form of people impersonating the owners, Julia, Timmy or Owen. The best way to avoid this scam is to double check that anyone who DMs you is actually the real person. **Our owners and developers will almost never DM people out of the blue, and will never ask you to screen-share.**



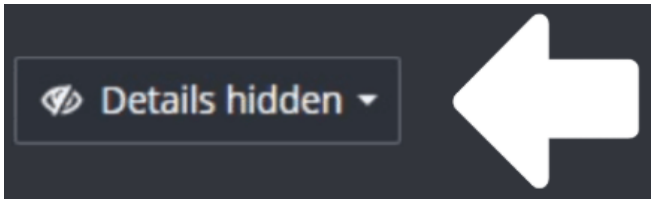
Game Testing Scam:

This scam has emerged recently and usually comes in the form of someone impersonating a well-known developer and asking you to test their game. In the example below, the user impersonated a Hokui developer and asked them to download/run a file which was supposedly to “test their game”. It goes without saying that you should never download files from random people, regardless of whether you think they’re well-known developers. **Always check that someone is who they say they are.**



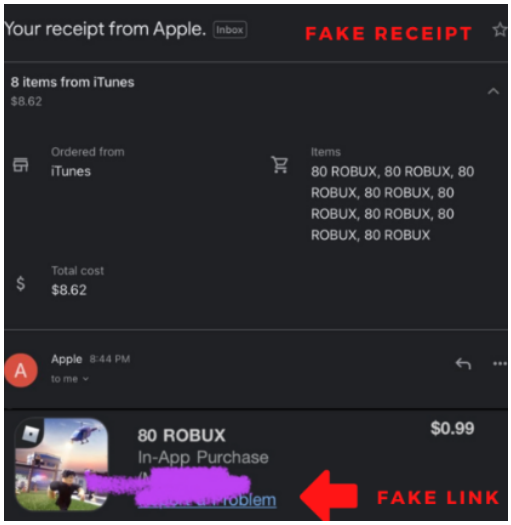
Gyazo Scam:

This scam involves the scammer DMing the victim for a Gyazo screenshot of the Roblox password reset page. They then pretend they can’t see the picture and will ask you to turn on “Details”. This option will give the scammer the ability to see where the picture was taken, and they can go to the password reset link to steal your account. To avoid this scam, always make sure your Gyazo screenshots are set to “Details hidden” before sending the link to them.



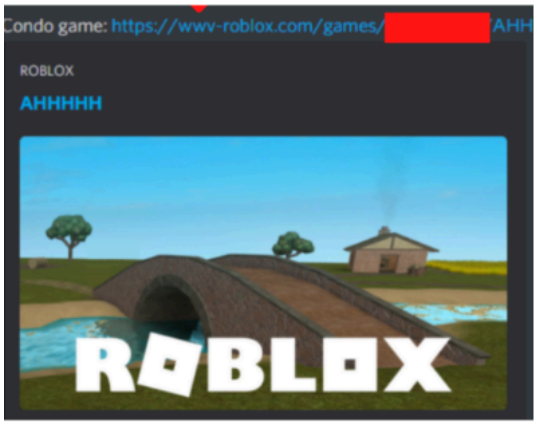
Fake Email Scam:

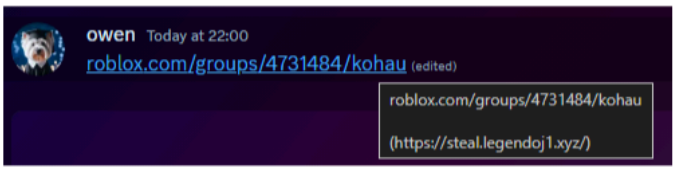
This scam involves you receiving a fake email impersonating an Apple/Roblox Support representative. They send you a fake receipt to make you think someone is on your account buying Robux. When you click the “Report a problem” link, your account will be stolen. Always make sure your emails are from official support accounts (support@roblox.com).

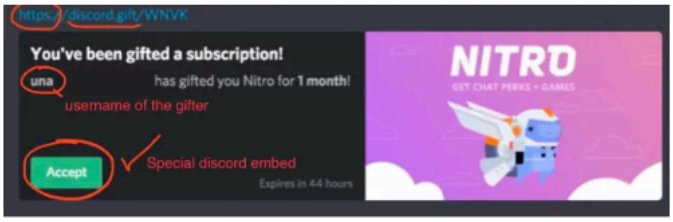


Cookie Logging and Phishing Sites:

This scam is the **most common one** - someone sends you a fake link and you click it. The site usually takes you to a page which prompts you to log in to your Roblox or Discord account. It can come in the form of a Roblox game, fake steam gift card link, fake nitro gift, etc. Don’t click links, even when they look real, and don’t trust something that’s too good to be true, such as someone sending you free nitro for no reason.

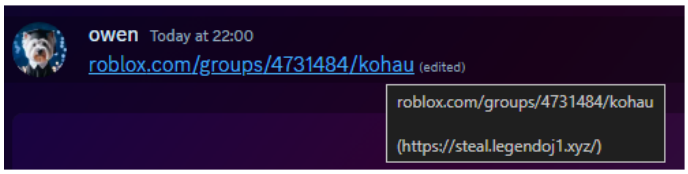


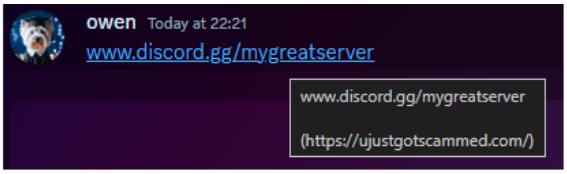




Misleading Links:

This is basically a “part 2” of the scam above. Using Discord’s Markdown syntax, users can hide malicious links in plain sight by disguising them as real links. Hover over links to see if they’re legitimate. Better yet - don’t click links regardless, especially if someone sends you a link out of the blue.



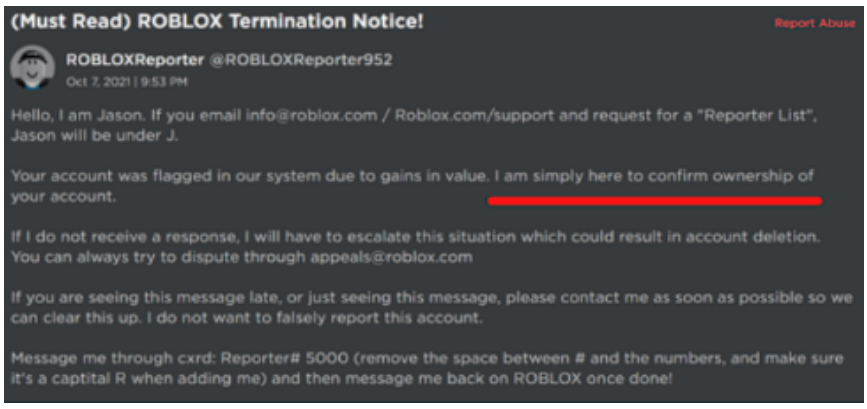


Fake Browser Extensions:

On the Chrome/Edge/Firefox store, you may have noticed fake Roblox extensions that will ask for the permission to “Access data for all websites” and “Read and modify your browser settings”. Some extensions may not even ask for this permission but will still have the ability to read and change data. Always make sure you install real extensions **(look for the verified badge)** and refrain from giving any extension access to personal data.

Fake Roblox Staff:

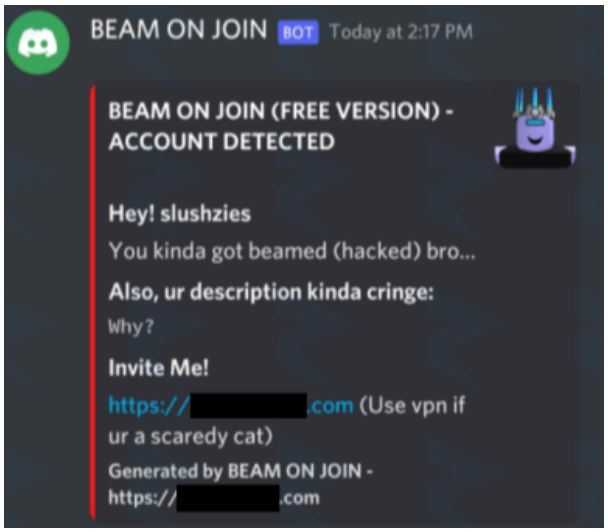
This scam is simple and similar to the developer impersonation scam above. A fake Roblox Admin account messages you on Roblox saying you were flagged for termination. They will ask you to add their Discord, and add their email account to the forwarding link. If you do this, this will send them every email you receive, including 2FA codes and password reset links. **Roblox administrators will NEVER message you on Roblox.**



Cookie Logging Discord Bot:

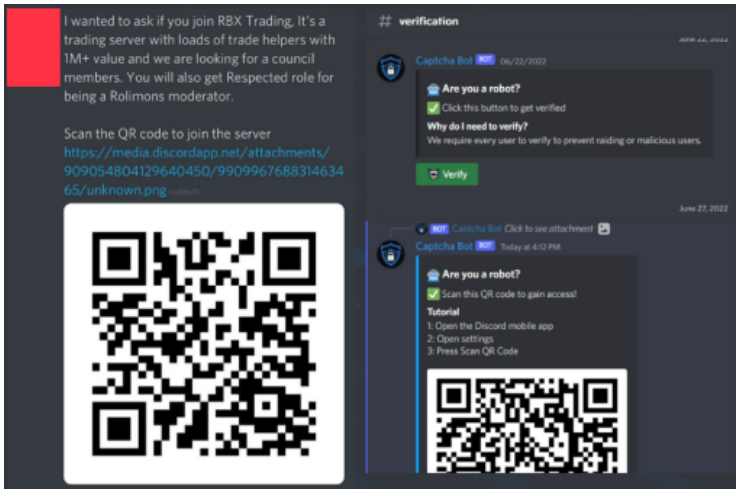
This scam method involves the scammer sending the victim an invite to a “trading server”, which upon joining, will prompt a bot to send you a DM saying you’ve been

hacked. This is an attempt to social engineer you into panicking and clicking the link to get your account back. Don't believe what random people tell you on Discord, and avoid joining suspicious servers sent by untrusted individuals.



QR Code Scam:

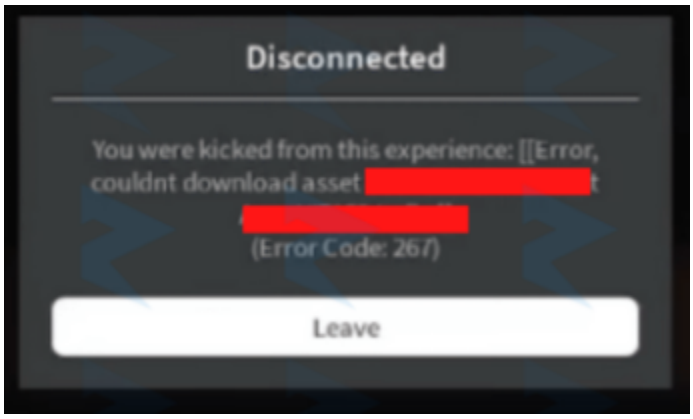
This scam method involves the scammer sending the victim an invite to a "trading server", which upon joining, will ask for a QR code to access. If you scan the QR code, your Discord account will be stolen. Don't join suspicious servers and don't scan QR codes sent by any person or bot. **No legitimate bot or user will ask you to scan a QR code.**



Roblox Account Termination Scam:

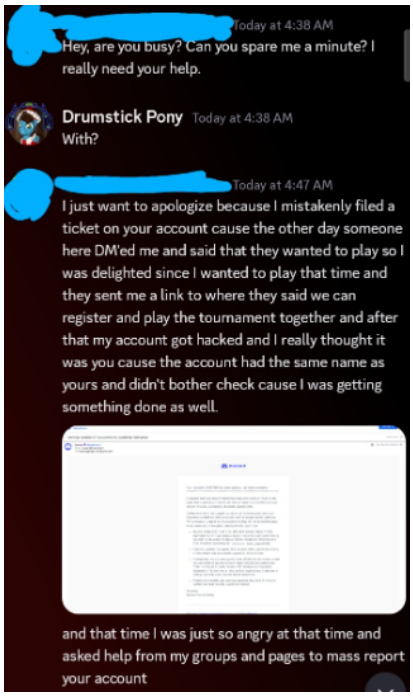
This is more of an exploit than a scam, but Roblox won't help you get your account back if you fall for it. It involves someone sending you an invitation to test out their Roblox game. It seems legit upon joining but you are kicked after a few minutes.

What's actually happening is that the chat script is being exploited to make you say bad words (that you can't see), which will get your account terminated. Don't "test" random games that people DM you or you will get banned and will struggle to appeal.



Mass Report Scam:

This scam involves the scammer messaging the victim telling them they have accidentally mass reported their Discord account. It is followed by them asking the victim to email or DM a "Discord Admin" to explain the situation. The fake Discord Admin account that the victim adds will send a link or ask for details that will allow them to steal the user's account.



If there's a scam that you've seen at Kohaú that we haven't written here, please DM details of it to Owen @legendoj1 on Discord.

Credits to Rolimon's and popeeyy for some of the scam screenshots above.

TRUSTING FRIENDS = ACCOUNT ENDS:

Whilst it may be quite a straight-up title, it's true: if you trust everything your friends send to you, you're putting yourself at a huge risk of account theft. In fact, the majority of account theft that happens at Kohaú is because people trusted links that were sent to them by their friends, even though their friends' accounts were hacked and sending them malicious things.

Just because someone is your friend, doesn't mean they can't get hacked too. If someone wants to hack you, they may target your friends first if they're easier targets. Make sure that you always double check links and files that you get sent by friends before clicking them. **Remember, if something is too good to be true, it probably isn't true.**

WHAT HAPPENS WHEN YOU GET HACKED:

If somehow after reading this guide you still have an "oopsie" moment and get your account compromised, here's what to do to try to get it back:

- If you can still log in to your account with your password, **login and change your password as soon as possible**
    - Once you've changed your password, every device where your account is logged in will be logged out
    - Log out of your account then log back in - this will reset your cookie so anyone who cookie logged you won't be able to access your account anymore (same goes for Discord)
    - Check what devices your account is logged in on (you can do this in Roblox/Discord settings) and log out of any device you don't know
- **Try to click "Reset Password"** - the hacker might not have changed the email and you'll still receive a password reset link in your inbox
- If you can't log in to your Roblox account, report it to someone in Staffing using your Discord account.

- If you can't log in to your Discord account, the best thing to do is get Staffing's attention. Create a new Discord account and verify with Bloxlink on your main Roblox account to prove it's really you. Then DM someone in Staffing who will ask you questions.

If you find yourself completely locked out of your account, you can report your account as hacked using the Roblox Support Form or the Discord Support Form, depending on the account.

CONCLUSION:

It's important that you stay alert and use common sense when dealing with potential account security risks. This document will be updated regularly with the latest scams to keep you aware of what to watch out for. **The biggest thing is to not click on links** - if you don't click on anything anyone sends you, your chance of being hacked is close to zero. Take the steps to secure your account and refer back to this guide if you ever get sent something that looks fishy.

Signed,
Kohaú Corporate Department

🔗 *Back to Document Portal*