How to keep your account secure.

	Facebook has a range of security features users can activate to better protect their account.	**Twitter has security features users can activate to help protect their account.**	**Gmail has security features users can activate to help protect their account.**
		Login verification (Two Factor Authentication)	2 Step verification
		For more information on keeping Twitter safe go to: https://support.twitter.com/articles/76036-safety-keeping-your-account-secure	For more information on 2 Step verification go to: www.google.com/landing/2step/
Built in Security Features.			
	Login approvals (Two Factor Authentication) Login notifications One time passwords Trusted contacts For more information on these Facebook security features go to: http://www.facebook.com/help ->Security -> Extra Security Features		
	You cannot access your account with your normal login credentials.	You cannot access your account with your normal login credentials.	You cannot access your account with your normal login credentials.
How do you know if your account has been hacked.	There are posts on your news feed that you never posted. These posts encourage your friends to click on the links.	There are Tweets from your account that you didn't personally make.	People receive emails from you that you didn't send.
What to do if your account has been hacked.	Clean your computer from malicious software before changing your password	Clean your computer from malicious software before changing your password	Clean your computer from malicious software before changing your password
	Scan your computer for any malicious software and make sure your antivirus is up to date	Scan your computer for any malicious software and make sure your antivirus is up to date	Scan your computer for any malicious software and make sure your antivirus is up to date
	Do not change your password until you are certain the computer you are using is free of all malicious software	Do not change your password until you are certain the computer you are using is free of all malicious software	Do not change your password until you are certain the computer you are using is free of all malicious software
	If you still have access to your account change your password (have a look at Password management)	If you still have access to your account change your password (have a look at Password management).	If you still have access to your account change your password (have a look at Password management)
	If you do not have access to your account, reset your password by clicking on the Forgot your password link on the log in page	If you do not have access to your account, reset your password by clicking on the Forgot your password link on the log in page.	If you do not have access to your account, reset your password by clicking on the Forgot your password link on the log in page.
	Remove any third party applications that you installed on Facebook.	Notify all your friends that your account has been hacked and that any suspicious tweets are as a result of the hack.	After taking back your account, notify all your contacts that your account has been hacked and that any suspicious emails they received are as a result of the hack.
	Report a compromised account. Go to www.facebook.com/hacked After getting back control of your account, notify all your friends that your account was hacked and that any suspicious posts are as a result of the hack.		
More Information.	www.facebook.com/help ->Hacked Accounts	https://support.twitter.com ->Troubleshooting	https://support.google.com/ -> Gmail -> Account -> Security & Privacy -> Gmail -> Security Checklist