



SMARTER THAN FACEBOOK SCAMMERS

**THE COMPLETE FACEBOOK SECURITY
HANDBOOK**

Written by James S Tolson and Chuks Amobi

Legal

All trademarks and intellectual property are the property of their respective owners.

Limit of Liability/Disclaimer of Warranty:

While the author has used his best efforts in preparing this material, he makes no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or any written sales materials.

The Publisher has strived to be as accurate and complete as possible in the creation of this report, notwithstanding the fact that he does not warrant or represent at any time that the contents within are accurate owing to future updates by Facebook.

The advice, guides and strategies contained herein are intended to guide one to tightening one's privacy on Facebook for personal and educational purposes. This material is not intended for use as a source of legal, business, accounting or financial advice.

Facebook is a registered trademark. This book is not affiliated with to future updates by Facebook in any way. Facebook does not endorse this book or anything this author says.

Introduction

How far!

I'd first like to thank you for purchasing this book.

You are AWESOME.

Security is a priority for everyone. It's people like you that make creating these information to help people worth it.

My name is Chuks. James and I have put together this guide to help people having challenges with Facebook security and compromised privacy. We have dedicated our experiences on Facebook and internet security into creating this guide just for you.

The only thing I would beg of you is to take time to read every words we have compiled. It doesn't matter whether you have come across them or not but there are vital things you may not have seen somewhere.

These are secrets most people are not willing to share in order to save misfortunes, suicide attempts, heartbreaks, strokes and other related mental disorder.

In case you come across any difficulty, please feel free to send us a mail via books@chuksguide.com and I will be very pleased to reply you as soon as possible. You can check our related great articles on our blog at www.chuksguide.com

If you think that this handbook is worth more than ₦5000 (which is originally ₦9000), you could cheerfully donate to us.

This book is bound to mistakes and grammatical errors. We would accept your kind corrections anytime.

A little insights about Facebook Security Loopholes

Facebook is so massive that they find it difficult to deal with every stored and incoming data on their server. It is more than a 2 billion social network with greater percentage of a single-user multiple and fake accounts respectively. It is commonly the case of online social networks and dating platforms.

It is a huge challenge for Chad Greene, director of security at Facebook, to maintain the trust and information of every single Facebook user by detecting and responding to threats to their personal life.

This handbook covers two things. They are Facebook account compromising or what we call hacking and Facebook scams. It is quite a broad topic no one could cover in a few pages. That is why we compiled more than 40 pages of useful guides to standing against these online security threats especially on Facebook.

I would like to give you three eye opener stories that happened earlier this year 2018. These are not stories I copied from NairaLand nor Linda Ikejis blog. The victims are my close friends and my younger brother. I can give you the chance to hear from them if you wish to verify. So pay attentively.

Here are the stories;

1. Hacked Facebook account

I had missed calls from my friend in one morning which is something unusual as a result of his busy morning work routine. I quickly called back because I perceived that “water must don pass Warri”.

The first thing he said was “....my Facebook account has been hacked and I can’t change my password”. When I asked what happened, he said “I logged in to with my Facebook for one job like that.

Here's what really happened;

His friend's account was hacked. What the hacker did was to send him a link to a job vacancy post on Messenger. At first, he thought it was from his friend not knowing that he wasn't chatting with someone reasonable. So he quickly clicked on the link to the job website. He was asked before he could read the whole job description, he has to sign up.

The only sign up was with Facebook which I know most of us do out of our laziness. Being someone in a haste, he just signed up with Facebook details with an interface that looked 100% as Facebook.

The summary is that

- a) The Facebook page he thought it was Facebook was a scam. They call it a phished page which we will discuss later in this book
- b) The username and password he used for his so called sign up was not collected by Facebook
- c) The username and password was simply submitted to hacker's side not Facebook.
- d) Finally, his account was taken over

But luckily for him, we got it restored back. He was simply fortunate enough. An account he created in 2010. It is not easy to come by an old Facebook account. It has respect.

We should be careful with what links people share to us on Messenger, our Timeline or being tagged to even if they are our loved ones. Many things do happen.

Note: I don't have images to attach because we only talked on phone

2. A Brutally hacked Facebook account

Another Facebook friend of mine account was fatally compromised by someone she doesn't know. She was sad because she's the type that uploads 20 photos in a go. That was her pain point.



The mistake she did was creating a new account, telling her friends to post on her timeline and broadcast that her account was hacked. That was really a bad idea. If someone has criminals as neighbor, the worst action is coming out to say “All these thieves, I have heard enough of you in this compounds. I’m just warning you to avoid complication”.

It is safer to stay mute and do some smart silent calculations on how to handle them. If police comes to your street and eventually book them even when you did not invite the police, they will eventually come after you. **It will be bloody.**

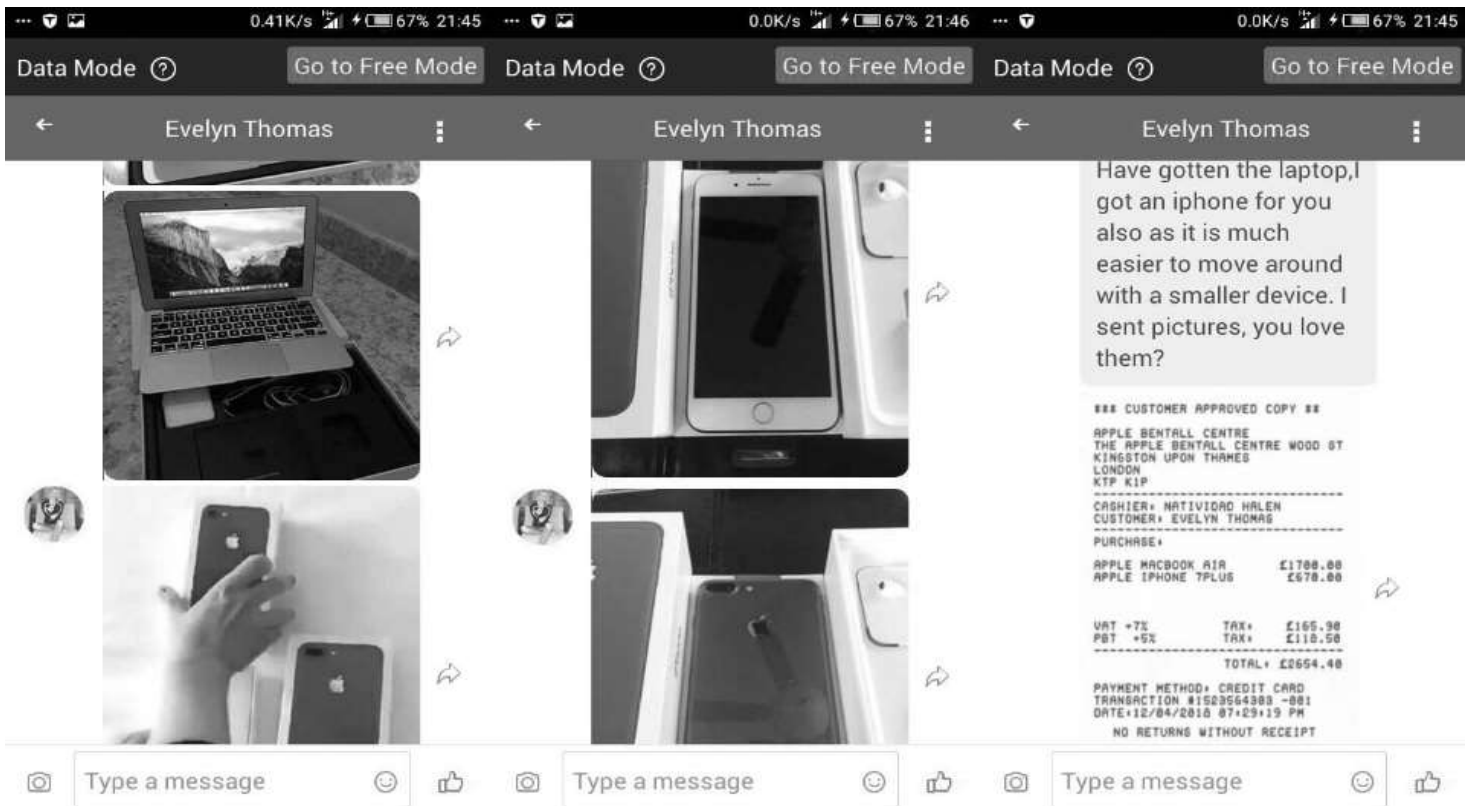
The hacker after seeing all the noise on the account quickly changed her profile picture, name, email and phone number. That was an operation Python dance 2.

The reason her Facebook account was hacked was not because her password was as easier than ABC. She used numbers as password which takes less than 60 seconds for a hacker to break. The main problem was because she failed to encrypt how her account will be accessed in future.

Later in this book, we have discussed 6 login security features that can protect one's account even when the password is just "preshbaby95" or a phone number. But it is not a good security practice. Learn to use a strong password.

In summary, she couldn't get back her account as a result many people reported the account and Facebook deleted it. We need to be wiser in the way we approach some security challenges like this even in real world.

3. An attempted smart scam

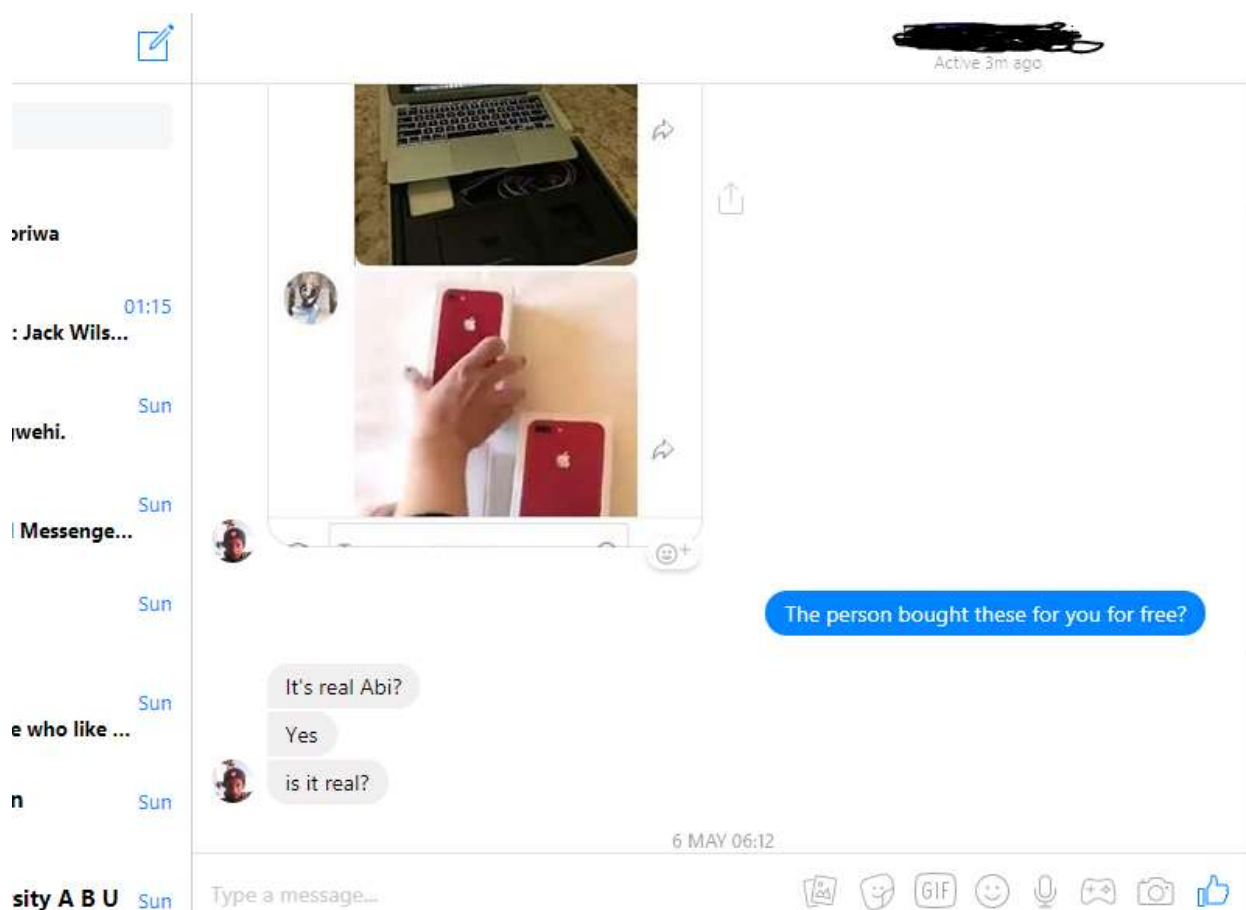


This was actually attempted on my younger brother. As younger boy's blood dey hot, they want to hook up with beautiful white ladies. But not everything you see as white are actually white, most are just Albinos.

My brother actually needed a PC and also to change his phone too. Meanwhile, the oyinbo lady sent him a friend request which is not really common. They just started flowing to the extent of him using her photo as his profile picture.

That's romance gone beyond beyond. She promised to buy my brother an iPhone 7S, a MacBook Air worth **₦1,106,718**. That was an unexpected assurance. He was quite too excited. You would do the same. Everything looked so real plus the receipt and white hand holding the iPhone.

To cut the story short, she asked him to send him a shipping fee that she has ran out of money at the time. She has to send the package tomorrow with a trusted Freight agent to avoid missing item. My brother has no such money and that is why he came to me.



At first I know it was a scam. I have to calm him down on phone to let it go. Many of these happen to lots of people on Facebook every single day. I am not emphasizing. I know what I say and I do.

I wouldn't forget to add betting scams that are too rampant nowadays. It happened to another close friend of mine. He was scammed of fake odds and immediately was blocked by the page. He had to create a new account and was also blocked. He created another and then swore to take the matter to the next level.

Here's what he used;

- He will send messages to the fans and people commentating on the page that he was scammed
- He will take the matter to a baba that's a good friend to his dad.
- He will torment not only him, but his entire family.

In less than 2 hours, his money was returned sharp sharp. You can see photos of won games and even testimonials but the truth is that they are doctored. Comments are either from fake new accounts or fellow scammers. Don't fall for any of them.

A lot of Facebook accounts are compromised every single day but how to deal with them is a big challenge. Facebook security team has promised to combat this threat during the Cyber Security Awareness last October. They have urged users to stay vigilant and report scams when necessary.

But will that really put an end to this?

One problem about Facebook and its users is the ambiguity of its features. Not everyone knows how to use Facebook the right way in regards to privacy control and security. Facebook has introduced post and profile reports but there are still some challenges to it.

One of the problem of reporting a post or profile to Facebook is that most of them take longer time before they are being acted upon. Even when acted upon, sometimes nothing can be done.

Another funny part of reporting a profile on Facebook turns out to backfire on the victim. Sometimes, after these Facebook hackers must have taken advantages of the account to promoting their contents, links, personal information, they now open a report case against the same account which eventually triggers Facebook blocking them.

But that sucks!

Protecting one's Facebook account

Facebook has come up with varieties of good technologies to help fight insecurity on their user's information. You might have come across few of them or currently using them at the moment but they may not guarantee your account from being compromised.

Here, we have highlighted several methods to help protect one's data on Facebook. They are categorized into sections and sub-sections;

- 1. Facebook Scam report system**
- 2. Facebook privacy control**
 - a. User login security**
 - b. Personalizing one's Facebook account**
 - c. Facebook Anti-Social Engineering**
- 3. Advanced and futuristic Facebook security**

Facebook Scam Report System, FSRS

In USA alone, there's a frequent reported scams costing *roughly \$50 billion each year* and are mostly through phone calls, social media and emails. More people are becoming victims on Facebook which was the case of Shellie as we earlier mentioned.

One expert estimates that at any one time there may be 25,000 fraudsters online with victims. One company that screens profiles for dating companies says that 500,000 of the 3.5 million profiles it scans every month are fake. Better Business Bureau (BBB) estimates that there may *be more than a million victims* in the U.S. alone, and they may well be people we know.

As you know, scams can happen anywhere at any time. Facebook as a multi-billion social media platform, people you had no idea about resides in your friend list and most of them follow your account without you even knowing.

Experts warn that someone could learn a lot about you by gaining access to all that's on your profile, like your status updates, location, date of birth and photos. Study revealed a massive number of fraudsters are using Facebook to gain unsuspecting people's trust to steal their money.

The scheme sometimes takes months to build a trusting relationship before the scammer asks for money, usually for an emergency or transportation, from the person they have conned into a relationship.

When they eventually walk up to you through Messenger as Messenger always prompts newly accepted request to say “Hello” or “Wave”. They try as much as possible to develop a good relationship with you. They are not doing this for Facebook connectivity sake rather for their own devastating interests.

They are always patient to collect every single personal details about you, including family, residence, your work status and income until they counter strike.

Facebook has combined automated systems led by Bill Slattery to detect, investigate and remove both suspicious and reported scams. But Facebook may be too slow before the scammers go away with your money or personal information.

It is required that you stay vigilant upfront and report any form of suspicion to Facebook without relying on its automated systems. Be careful with the type of friend requests that one accepts.

On Facebook, scams begin with scammers creating fake accounts or by hacking into existing Facebook accounts or Pages you've liked. The fake accounts always take either the identity of public figures, politicians, military members, sexy faces or people you trust. Scammers use these fake or compromised accounts to trick you into gaining your interests.

If you get a friend request from an existing "friend," verify that the request is genuine before accepting it. And of course, be very wary of friend requests from people you don't know. They can also send messages to your friends, posing as you, in an effort to learn more about you, ask to borrow money or try to meet up with your friends.

One could actually end up interacting with an imposter who had used his name and profile picture to create a profile. One's account could get hacked and then be used to manipulate the victim's friends and friends on Facebook.

Facebook scams can come in these ways;

Phishing:

This has recently been one of the commonest scam to watch. Facebook is so open and gives access to developers to integrate their apps into its platform. Being so common to most developers, the bad guys now take advantage of it to inject scripts into creating automated fake accounts.

These automated fake accounts are handled by hard core developers. They are either paid for the service or as part of their project. What they do is to define the accounts to target specified demographics – *sex, age, location, interest and page likes* to be used with their fake account generator.

After a fake account is generated, it then forwards fake friend requests to the targeted demographics above. If you are ignorant of behind the scene, you will definitely click **Accept** button. But if you are the type that is reluctant to accept friend requests, Facebook automated system will delete them within 48hours.

Let's say that you already accepted the friend request, there are key things to know about auto generated fake accounts;

1. It has at most 2 photos which include 1 profile photo and 1 upload.
2. The profile photo always looks good to be true usually that of a model, soldier, business person or even half naked woman. Men have quick arousing appeal to great looks.
3. The Facebook account is usually less than 24hours old with almost no contents.
4. Even when there is a content, it should redirect to an external link either to see a nude video or "watch me on live cam" video.
5. You have no mutual friends.

Their aim is to drive people to their suspicious links to watch them naked or perform some information sharing in a bid to win a prize. Assuming you accepted the request, went straight to their timeline and eventually saw an arousing photo urging you to see more of that by clicking a link.

When you click, you will be directed out of Facebook and your security is void. You might be charged less than \$1 to watch a girl on a cam which I know most men would be happy to spend for that great opportunity. They will just zap all your dollars in seconds.

The photo below shows a fake account as Wendy Griffith in search of a strong and funny man to heal her broken heart. This is a nice caption in addition with the charming photo that no man wouldn't dare to resist.

If you could check the name on Facebook right away, you won't find the profile again either because it might have been flagged or deleted by Facebook.



But the intention is not on your \$0.99 you will spend, it is just your credit card. You might be giving an option for PayPal which gives one the boldness to even spend more but they could just be a cloned PayPal website (phished PayPal website).

All they need from you is your PayPal login details. Once taken, they will stealthily redirect you to PayPal and that's GAME OVER. This type of finding romance as in the case of Wendy as in the photo above, she could really be interested in a long distance relationship that would put one in a messy situation.

For the case of winning a prize promo, you submit your name, email, zip code, home address for your prize to be delivered to.

Even if you are to accept friend requests, try your best to define the kind of people you accept. The best and the only option is usually friend requests with at least **five reasonable mutual friends**.

Here's what we meant by 5 reasonable mutual friends – If someone sends you a friend request and shares up to 10 mutual friends with you. Then, try to consider 5 persons out of their mutual friends.

If the 5 persons are friends you really know on Facebook which could be your real friends, family or some reasonable persons that you have developed good friendship with.

Then consider accepting those requests but if you find it difficult to identify the mutual friends you share with someone that already sent you a friend request, just delete them.

The recent form of phishing is job listing. A friend of mine's account was hacked because his friend sent him a link into his Messenger. The link leads to a job listing website that requires one to login with Facebook before they could continue with the job application.

It is so simple to login with Facebook account as long as the website has the plugin enabled. After some minutes he logged into the website, no content was found. Logging back to Facebook was another challenge. He has been logged out of his device. He called his friend to complain what happened to the link he sent him, guess what happened?

His friend was confused too. Someone else sent him the same message of which he opened. He was hacked too. The message might have come from the hijacker. You might be wondering how their account was hacked. The one reason why they were hacked was because the Facebook login they clicked was actually not Facebook.

It was a cloned Facebook site. This is called phishing. While entering their Facebook login details, their username and password was just filtering into the hacker's server in form of text file. They just submitted their details to them to immediately login to their account to take control. When trying to login to any website using Facebook, make sure that the address is actually <https://web.facebook.com/XXXX> or <https://m.facebook/XXXX>. Anything apart from this could be a phished website.

You can take a look at Z-SHADOW (<http://z-shadow.info/>) . This is what normal people use to hack someone's Facebook account. It works like a normal Facebook app we use daily like QuizStar and other funny apps we use to check how we will look like when we reach 40 years, how our child will look like and other similar Facebook app.

Once someone shares the link they created from Z Shadow either on their Timeline or Messenger, they pose as a security threat to your account. We have to open our eyes very well. For the type of people that wants followers on Facebook, more likes on their posts then they are the potential victims.

If you could run away from any link on Facebook, any apps on Facebook, you will be saved from this.

Social engineering using family or friend:

These are not people you know but they have studied every single social activity of either you family member or old friend. They either create a cloned account of them or better still hack into theirs.

Facebook is nobody's home. This is on a negative side to people that discuss every single thing about their family, relationships and work. It is over 2 billion people you have no damn idea about.

Everything in this category happens in twinkling of an eye. They study your conversation on your Messenger and patiently wait for the right time for the money.

Here's a lookalike sample of their message;

Good afternoon Joanna,

I just purchased this new Ferrari toy for my kid Scott for his birthday but my credit card isn't working on their payment. Today is their last day on promo before the price goes back to \$1000.

The price now is \$350. I will transfer you the money when I come back this weekend.

Love you ;)

The link; <http://buy-amazonn.com/products/baby-ferrari-toy?buy=10>

When you look at the sample, everything is so personal between them. It is because the scammer has studied their tone of conversation and their interval of conversation. She may not need to call her before making the payment because she is her sister/friend.

Another sensitive thing in this sample is the link to buy the Ferrari toy. It looks like Amazon and she will probably be too quick not to confirm if the link is really Amazon when there is already Amazon and the site is a carbon copy to Amazon.

They won't just charge you \$350, your credit card is completely at risk. So, you have to be careful about any link that is sent into your Messenger no matter who the person is. Don't allow people to tag you on posts that look too good to be real. Just untag yourself. It is simple!

Romance:

It is very difficult to give account of every person on one's Facebook friend list. These romance guys only want you to develop a deep interest in them. They usually pretend not to be in the same country with you or even continent as you.

But over the time of being on your Facebook list, he/she has known your financial power, interests, relationship status, likes and dislikes through what you share on Facebook.

In order for them to win your heart, they will always be the first to like or comment on your posts, send you the best birthday wishes, redirect posts that you will love, last to send you goodnight chat, first to wake you up, send messages in an adorable manner until you couldn't control your emotional interest on them. They virtually appear to be genuine.

Their goal is to build trust with you over time with the hopes of receiving money for personal aids, emergency, phones, notebooks, flights, visas either to come join you or complete some challenges. They wouldn't want you to come see them but just for them to come to you. They keep receiving money from you till you have no other way to get the money.

Anatomy of a Romance scam

Professor Monica Whitty in the UK has studied the psychology of romance frauds and found that they develop through several distinct stages.

First, devising an online profile and making contact with vulnerable victims. Second, developing a trusting relationship by isolating and grooming the victim, learning as much about the victim's family, background, dreams, and assets as possible. Many of these tactics are similar to those used by predators of human trafficking and online child pornography.

Third, they find a way to get the target's money. During this process, they also may use these victims as money mules to process money for other frauds. Finally, many times the same people are re-victimized after they learn they have been defrauded.

How do they contact victims?

The romance scammers operate on dating websites, but sometimes use **Facebook** and other social media. Obviously, scammers focus their efforts on those most likely to be interested in the "relationships" they offer.

On Facebook groups, especially dating and relationship group, almost one quarter percentage of the members are fake accounts which are usually as a female profile account.

One of them is [DATING GROUP, Netherlands, Canada, Pakistan, US, UK, UAE.](#) There are lots of similar groups on Facebook. Some desperate relationship type have been scammed from these fake accounts while others were able to figure out that they are just hungry scammers.



Who do they pretend to be?

Those engaging in online romance frauds try to build personas of people that they think would best attract the opposite sex. For women, they typically claim to be men that are financially stable, such as business owners, Professionals that work internationally or soldier.



Lucia Bella Williams ▶
DATING GROUP, Netherlands, Canada, Pakistan, US, UK, UAE.
18 February at 23:37 · 🌐

I'm new at this online dating because i was introduced to it by a friend and I need a serious relationship here no fake please... Hangout only:
luciawilliams008@gmail.com



👍❤️😱 444

120 Comments · 4 Shares



Watch out guys hangout is a sign of scam ooo hmmm



Princess Salma is 😊 feeling positive at 📍 South Beach, Miami. ...
24 December 2017 · Miami Beach, FL

Any takers?? Single here

I want true love ..unconditional love



It is also common for the profiles used to claim a strong religious faith, denoting someone with strong values and, thus, solid and trustworthy.

How can you tell if someone is dealing with scam?

There's no special identifier to any scam activity. Sometimes it could be very difficult to identify them from onset especially when the victim is damn desperate for either finding a date or life partner.

If you meet anyone on Facebook, and for some reason cannot meet in person, video calls but requests money, there is a very high probability that it is a fraud. Do not loan or give personal identifying and financial information or send money to someone in an online romance or over the phone.

If someone could take off your conversations from Messenger to Hangout or Email, something could also be wrong. When such happens, try to be smart and cut off. Engaging with the scammer to test their credibility may not work because they do this every day, they know how to respond.

Report the account to Facebook then block them straight away. Make sure that you have gathered some information which are totally untrue but it will help since they repeat the same template to all their victims.

Here are some things you could do before blocking them;

- Google the photos being sent to you. You will likely see a different name. You could use Google chrome or tineye.com
- Search some or most portion of the messages he/she sent to you. There's a possibility that they have used it on another platforms and persons.
- Use the State Department to transfer funds for an emergency. [Learn more here](#)
- Check to see if someone in the military really needs money. [Click to read more how it works.](#)
- Apply for Facebook ThreatExchange program
- Report scam at Scam Watch <https://www.scamwatch.gov.au/report-a-scam>

Lottery/Win a prize promo:

Lottery scams are often carried out from Facebook Pages impersonating an organization, brands or celebrities. The messages will claim that you're among the winners of a lottery and that you can receive your money for a small advance fee.

The scammer may ask you to provide personal information, such as your physical address or bank details.

For a win a prize promo, you may have seen something like

“Range Rover is giving a brand new Range Rover Sport on their 10 years anniversary. To win, share this post, then click on this link to submit your details for the raffle draw”.

“Apple is giving out a new iPhone X, complete the survey to be in a list of winners”

Be wary of the following:

- People asking you to move your conversation off Facebook (typically another messaging service or Email).
- People claiming to be a friend or relative in an emergency - In these situations it's probably best to call that person before you respond.
- Pages claiming to represent companies, public figures particularly those who are not verified directing you to claim a prize celebrating their anniversary.

Facebook privacy control

This section is the bone of contention when it comes to protecting user's privacy – what they share on Facebook. It is grouped into four important sub-sections;

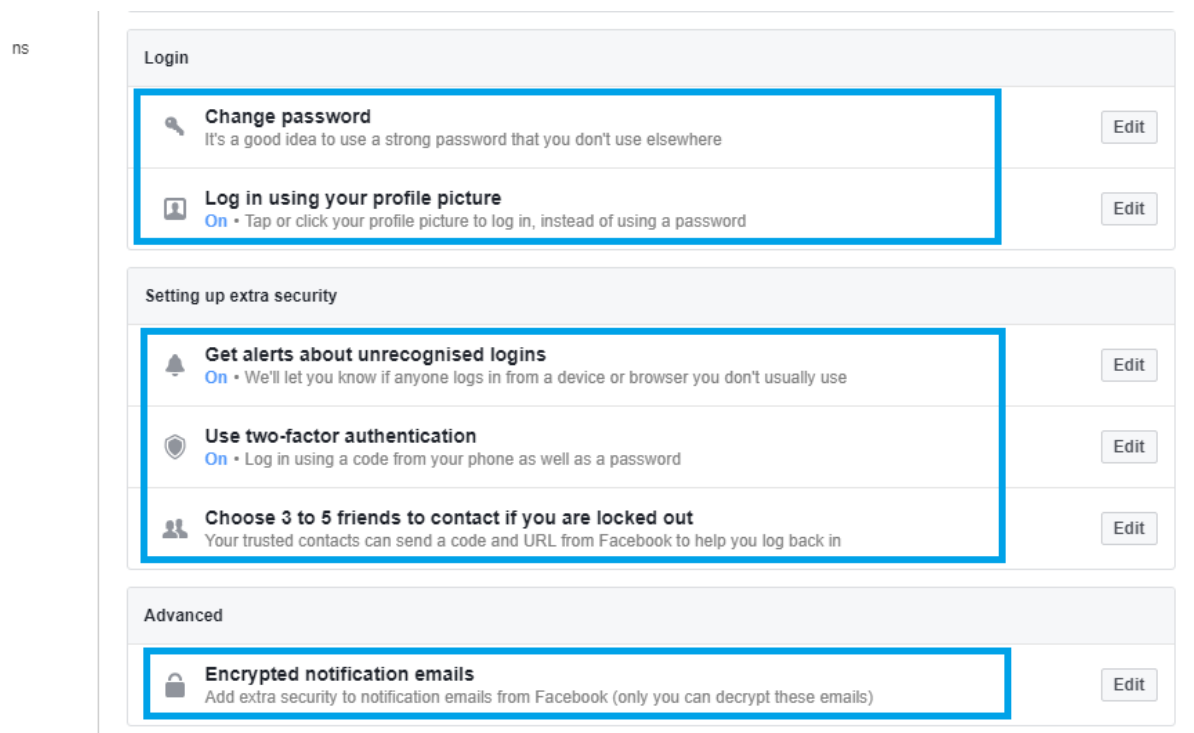
1. User login security
2. Personalizing one's Facebook account
3. Facebook Anti-Social Engineering

4. Prioritizing one's account

It is pertinent to understand this part very well because it will keep your Facebook account safe from hackers. Some of these options are already there on Facebook but this guide will walk you through to leverage their preferences on how your stuff are controlled on Facebook.

User login security

Facebook has changed the way in which one logs into one's account for safety reasons. They have introduced features like;



- Password change
- Two-factor authentication (originally named “login approvals),
- Where you're logged in (showing device, location, and login date and time for each place you're logged in)

- **Get alerts about unrecognized logins**
- **Choose 3 to 5 friends to contact if you get locked out**
- Login using your profile picture

They are a lot right? Yes! You may not need to enable all of these login settings for your single Facebook account. They all work differently.

Password change

It is recommended to always change one's online password at least 2 times a year. The reason is to break any connections to any hacking attempts. Also form the habit of using very strong password.

Best practices involve use of strange words, symbols including caps (vFrGC331c5H3EI, &M1LL13!, CH@rl13 Wo#D). Wrong password practices include English words, nicknames, pet names, phone number (janedoe, kyrian95, cynthia1996, charlie, millie, bonnie).

Our choice of password is usually the case of familiarity and memorable sake. Strong passwords determine the strength of your account and tells how difficult, number of days, years, and century it will take any prying eyes to sniff into one's account. Read this article on [how long it will take hackers to break your password](#).

Always remember to use a password you can never remember. If you cannot remember your password, how would someone else know it? The best thing to do is having a cloud password keeper – somewhere you can store your passwords and also be accessible anywhere. Dropbox, Google drive is a good idea.

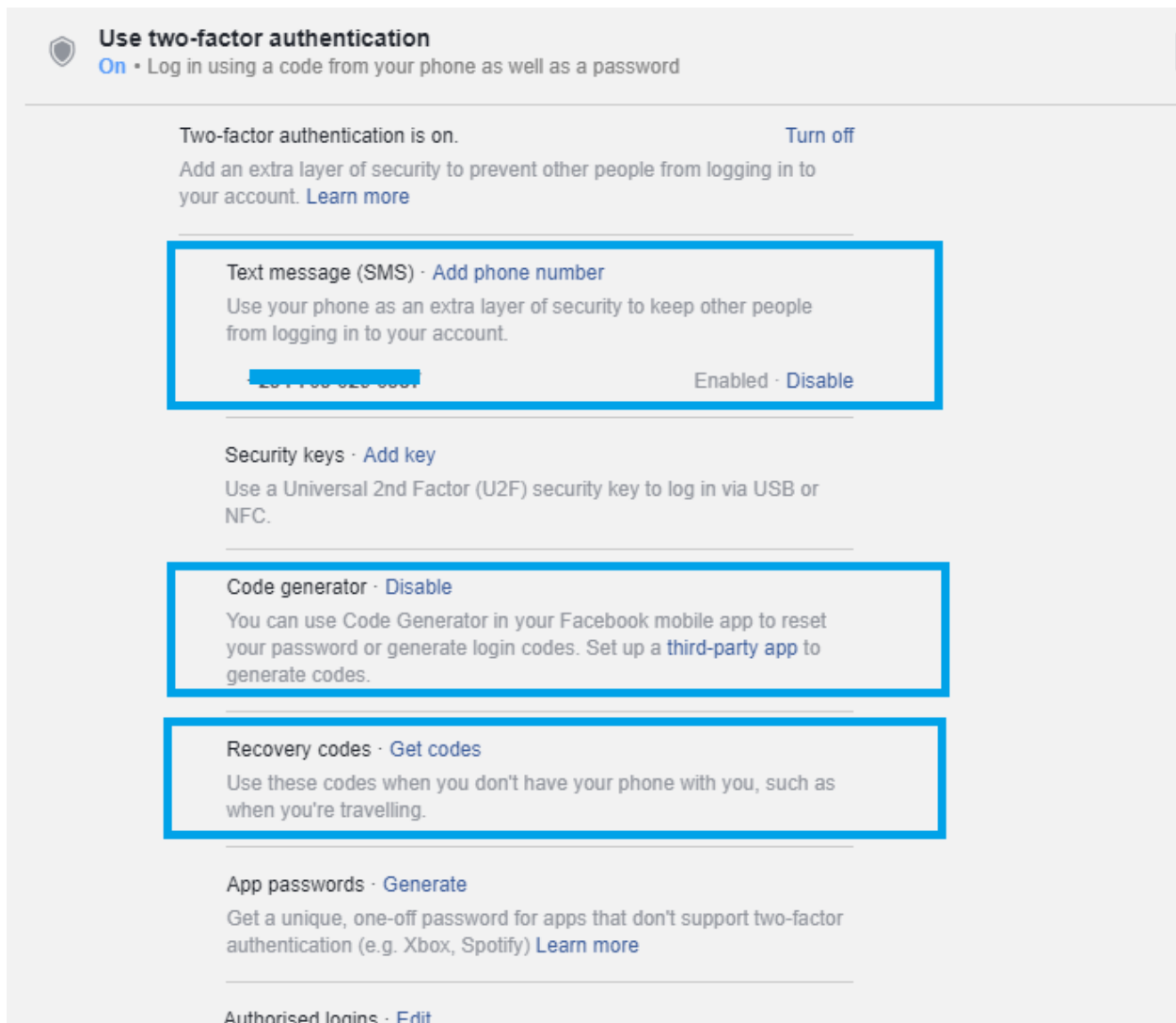
Two-factor authentication (originally named “login approvals”).

This allows one to add additional security layer to one’s Facebook account aside from the normal username and password. It is just like a cop calling for a backup team because he believes that his gun and bullet proof might not be enough for that particular operation.

That means when you log into Facebook from a new device or browser, you’ll enter a special security code sent to your primary phone from Facebook. That way, it’s much harder for someone else to access your account, even if they have your password.

In Two-factor authentication, it means that you want to approve any new or future login apart from where you are currently logged in. Facebook has multiple two-factor authentication methods.

Depending on which two-factor method one is using, it means that one has to authorize any new login from any device. Click [here](#) to choose two-step authentication or go to Settings – Privacy – Use two-factor authentication.



You don't have to enable all the two-factor method. You are only required to find a very convenient method that is simpler for you.

In this case, we have figured out only three out of five (3 out of 5) are suitable for any level of understanding. They are;

- Text message (SMS)
- Code generator and
- Recovery codes

Text message (SMS)

Here, Facebook allows one to enter and verify their primary phone number so that they can receive login approval codes usually a 6-digit code. Without this login codes, one cannot proceed with registering a new device to your account.

There are few things to carefully take note of;

- Make sure that a single phone number is attached to one Facebook profile account.
- Delete phone numbers that are not usable by you to avoid the case of our first story.
- Your phone number should be available at the moment when you want to login to your Facebook account in another device.
- If your SIM card is turned on for DND (Do not disturb), you may consider turning it off in order to receive sms from Facebook.
- If you are using a spam filter for SMS, you have to check spam filter messages also.

Code generator

Code generator is used to generate login codes. These login codes become useless within 30 seconds. That means in every 30 seconds, new login codes are generated until one logs in.

Code generator works on Facebook mobile app for Android and iOS. One can also use third party apps to set up code generator. But the bad side of code generator is that one may be locked out of their account if their first added device was on PC unless if text message is also turned on.

Recovery codes

Here, one has the option to generate login codes to be used to login with a new device. This is ideal for people that are not always with their phones or travelers.

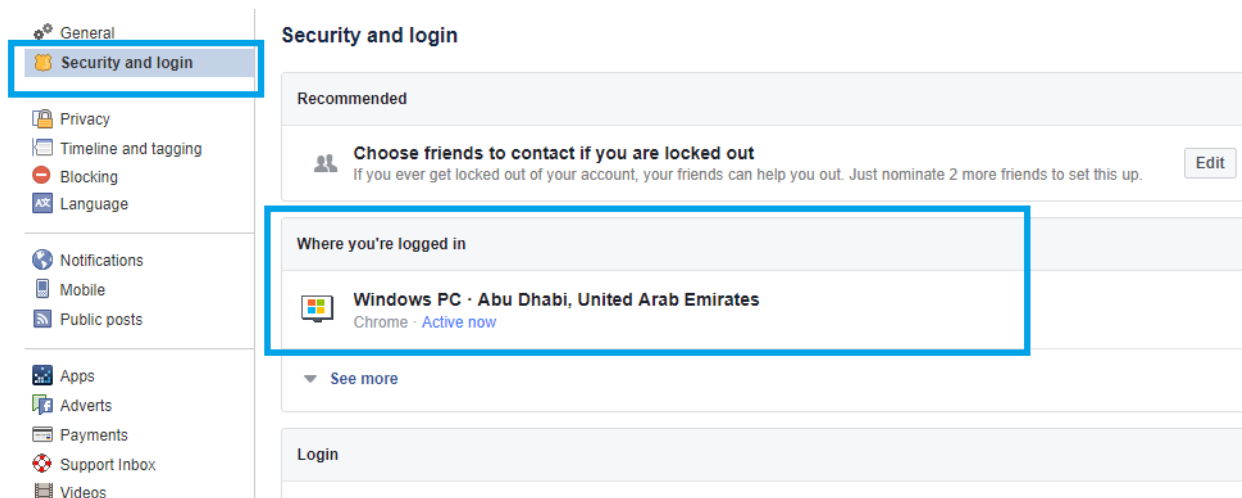
Facebook will give you about 6 different login codes to be used to login. You have to write these codes somewhere to be used any time one needs them.

What's the best option for two-step authentication?

Recovery codes is good but someone may displace where it was written. Code generator is also good but there are some challenges to average persons?

Now, text message sounds to be a better choice because everyone makes use of their phones with their primary phone numbers in it. Text message gives one the option to add more than one phone numbers.

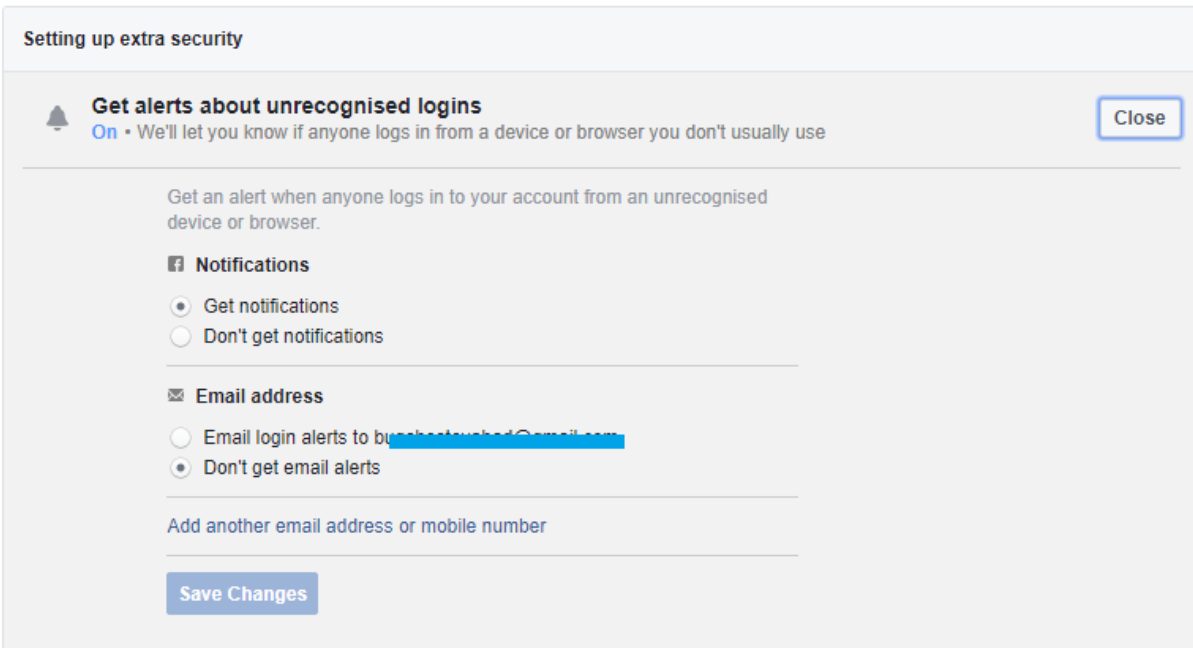
Where you're logged in (showing device, location, and login date and time for each place you're logged in)



The intention here is to monitor one's login activities on their Facebook account. In this place, it shows the list of logged in devices, their locations, IP address, date they logged in and time.

It is left for one to know if actually one did login in those places. If they seem too suspicious to believe, you either log them out or click **Not you?** To quickly change login details. Click [here](#) to review your login activities or go to **Settings – Security and Login**.

Get alerts about unrecognized logins



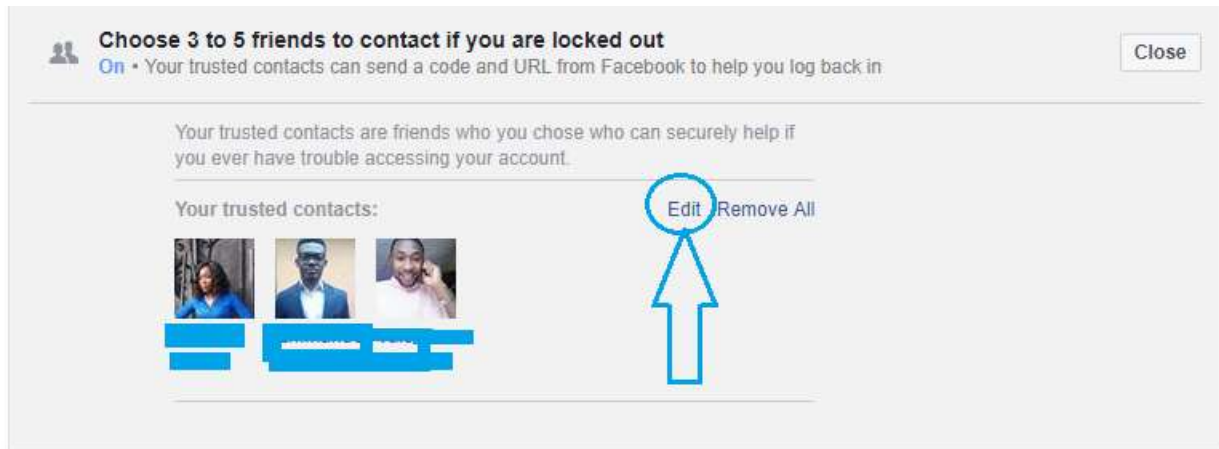
The screenshot shows a Facebook security settings dialog titled "Setting up extra security". The main heading is "Get alerts about unrecognised logins" with a bell icon and a status "On". A subtitle reads: "We'll let you know if anyone logs in from a device or browser you don't usually use". A "Close" button is in the top right. Below, a description states: "Get an alert when anyone logs in to your account from an unrecognised device or browser." There are two sections: "Notifications" with radio buttons for "Get notifications" (selected) and "Don't get notifications"; and "Email address" with a checked checkbox and radio buttons for "Email login alerts to [bunjabnabunjab@gmail.com](#)" and "Don't get email alerts". A link "Add another email address or mobile number" is below. A "Save Changes" button is at the bottom.

Facebook lets you know when someone logs in to your account from an unrecognized device or from a browser you don't usually use. You have the option to enable get notifications or not using either email or phone number.

With this, whenever you receive suspicious alert of recent login, you quickly move over to Facebook to change your login details. This feature is great to be enabled. Use this

[link](#) to enable get notifications or go to **Settings – Security and login - Get alerts about unrecognized logins**

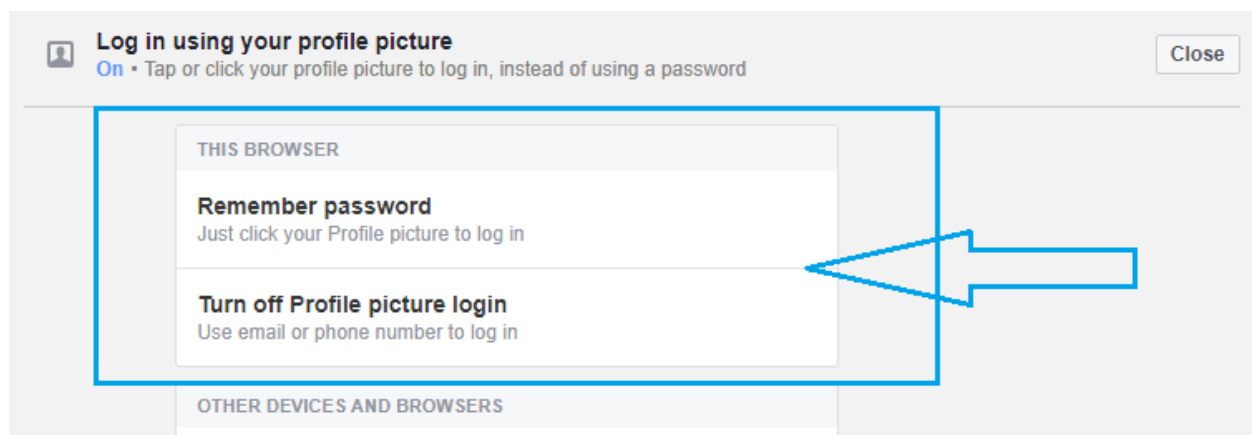
Choose 3 to 5 friends to contact if you get locked out



If you ever have trouble accessing your account, Facebook allows you to retrieve your account from your trusted contacts. These trusted contacts can be close friends or family. Their job is to send a code and URL from Facebook to help you login back.

One can have up to 5 trusted contacts. They all must be your Facebook friends. Click [here](#) to add your trusted contacts or go to **Settings – Security and Login**

Login using your profile picture



Tap or click your profile picture to log in, instead of using a password. This feature is available on Facebook for mobile and Web browser. You don't need to keep retyping username and password each time you log in.

But this feature is not really recommended if your device is too open to other people.

Personalizing one's Facebook account

Defining how information shared on Facebook are seen is a form of personalizing one's privacy. Facebook has features to control how information are controlled on its platform and outside its platform.

It is true that Facebook collects and tracks the activities of its user but they give one the full control on whatever one shares. It is left for one to personalize how his/her information – status updates, mobile uploads, contact details, bios, privacy and lots more, are controlled by Facebook system.

There are many ways to control how your information are displayed on Facebook, they include;

1. Through post's audience privacy using Who can see my stuff
2. Restricted lists
3. Custom and exception list
4. Blocking
5. Restriction on who sees personal and contact details (address, phone number, current city, family member, relationship status, work details).

The above ways have been discussed in details in a way to enable you understand their importance and level of usages.

Through post's audience privacy using who can see my stuff

Generally, there are few ways to control who sees one's post. This could be direct from one's post or coming over to Facebook privacy settings and tool as in the image below.

But the best way is to define the general setting through privacy settings and tools feature [here](#). This feature has sub-sections;

- Who can see your future posts
- Who can see your friend list
- Limit Past Posts - Limit the audience for posts you have shared with Public in the past
- Who can contact me
- Who can look me up

Who can see your future posts

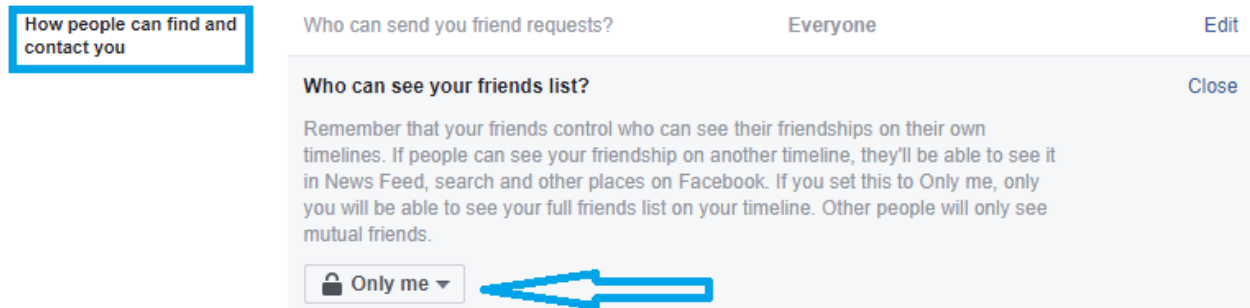


This allows one to set who will see one's post when next they post anything on Facebook. By default, Facebook audience privacy is set to *Public* meaning that everyone on Facebook that comes across your profile can see everything you have shared whether they are on your friend list or not.

When it is set to *Friends*, you are telling Facebook to only show whatever you share to only people on your friend list. For anyone to see your posts, they must be your friend in order to do so. But when it is set to *Only me*, nobody except you sees your posts. It is like you are just talking to yourself.

For the sake of this book, the recommended option is Friends especially if your account is a personal profile.

Who can see your friends list



One day, I received a comment on my blog saying “Please how do I hide my friends, people are starting to steal my Facebook friends”. For a while, I was speechless.

In my own Facebook account, I restricted my friends to ‘*Only me*’. This means that nobody sees the number of friends I have nor see their faces unless they comment or like my posts. That was for a personal reason which I will share to you now.

People have different reasons for sending friend requests. Maybe they want to get closer to your family, close friends, beautiful faces on your list. They may also want to clone their profile or decide to study their relationships with you. Everything on social media is quite complicated.

It is either you decide whether your friend list to be open to Public, friends or just you alone. In this case, I would say let it be just only for me.

Limit Past Posts - Limit the audience for posts you have shared with Public in the past.

How people can find and contact you	Who can send you friend requests?	Everyone	Edit
	Who can see your friends list? Remember that your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will only see mutual friends.	Only me	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit

Do you want search engines outside of Facebook to link to your Profile?

When this setting is on, search engines may link to your Profile in their results.

When this setting is off, search engines will stop linking to your Profile, but this may take some time. Your Profile can still be found on Facebook if people search for your name.

☒ Allow search engines outside of Facebook to link to your Profile

This is an extension of the first option, who can see your future posts. With this, it allows one to change the audience of all your past posts you have shared starting from your first post on Facebook to what option you chose in the first option (Friends or Only me).

This means, if you chose who can see your future updates to Friends, then all your past posts will be changed to Friends and vice versa.

Who can contact me?

This manages who will be able to send you friend requests on Facebook. It could either be Public or Friends of friends. Friends of friends are your mutual friends – they are the friends of your Facebook friends. I recommend you choose Friends of friends instead of Public unless you want anyone on Facebook and outside of Facebook to send you requests.

Who can look me up?

Here, you define who can find you on Facebook either using the email address you registered on Facebook, phone number or by simply searching your name on search engines.

You can restrict these options to only Friends. In the case of “**Do you want search engines outside of Facebook to link your profile**”, kindly choose **NO** if your account is strictly personal or otherwise.

The benefit of restricting search engines outside of Facebook to NO is to avoid one’s Facebook account ID being jeopardized by hackers.

There are tons of dark web forums on the internet. Some of these offer free Facebook account hacking by requesting to pull one’s account through randomizing Facebook ID. What they do is to input random Facebook ID into their hacking scripts.

If the account has allowed access for other search engines outside of Facebook to link one’s profile, then there is a chance that the account will be compromised.

Better still, someone can still target one’s Facebook ID either hovering around the person’s Facebook profile or using [findmyfbid](#).

Note: Facebook has disabled the option because Scammers abused Facebook phone number search.

Restricted lists

Restricted list is a special feature to filter friends that you don’t consider sharing some updates on Facebook with. From the name, restricted, any friend added into the list is restricted from seeing anything you post that is set for Friends audience.

Putting someone on the Restricted list means that you’re still friends, but that you only share your posts with them when you choose Public as the audience, or when you tag them in the post.

Most people will prefer to use restricted list on boss at work and family so that they can share anything on Facebook without them seeing them. They are not blocked.

For example, if you add your boss at work on Restricted list, then whatever you post on Facebook will be invisible to your boss as long as you set “Who can see my post” to “Friends”.

If your boss goes to your profile, they won't be able to see anything you have posted until you tag them or change your audience to Public.

With this, you can define who sees what you share on Facebook. There are posts meant to be for family, close friends and even strangers.

To add group of people on Restricted list, kindly follow this [link here](#) or go to Settings – Blocking then move to Restricted list.

To add someone on Restricted list, you can follow the below steps;

1. Open their profile page either using Facebook app or web browser
2. Head to the Friend tab and hover over the drop down
3. From the drop down, click Add to another list
4. Then click Restricted

If you consider removing anyone from Restricted list, then follow this [link](#) or go to Settings – Blocking then move to Restricted list.



Click Manage List in the top right, then click Edit List. Click on a friend's profile picture to remove them from your Restricted list.

Custom and exception list

This is a special form of Restricted list. This allows one to define who specifically sees one's post when shared. Unlike Restricted list, you can create custom audiences like family, close friends, course mates, coworkers and much more.

Exception list works almost exactly like Restricted list but it is dynamic. You can change whoever you want to be exempted from a post whenever you want to share your stories on Facebook.

The significance of custom list is to be specific in who sees your posts. Let's say your office had end of the year party and almost all the coworkers are on your Facebook list.

You can decide to create a custom list for coworkers and share the pictures you took at the party instead of tagging all of them in a single post. This limits the number of people that are not supposed to see what you share.

To create custom or exception list, tap on "What's on your mind", tap on **Friends** or **Public** depending on your privacy. Click on More...Then Custom. From here, define your custom audience. For exception, click on **Friends except**. Black list who you doesn't want to see your updates.

Blocking



When you block someone on Facebook, they will be unable to view your account, send you messages. Blocking is a great way to totally remove suspicious profile that comes across your Facebook account.

To block someone on Facebook, go to their profile and tap block. To block a number of people, Go to

1. Settings
2. Blocking
3. Then enter the Facebook names to block
4. Then Block

You can block anyone whether they are your Facebook friend or not.

Restriction on who sees personal and contact details (address, phone number, current city, family member, relationship status, work details)

This is one of the major weaknesses of victims of Facebook scams. People are always not too concern on how their personal information – phone numbers, email, home address, location, family, work, etc. are displayed on their Facebook profile.

By default, Facebook shows every details one enters during registration to Public. This is to give people the privilege to recognize your account on Facebook. But you can still decide on how you want your stuff to be displayed on Facebook platform.

Let me give you some insights on how scammers leverage on Public personal information. Assuming your phone number is visible to everyone on Facebook to see, they can look up your call records, WhatsApp information.

For email, they can sell it to spammers for promotions, hackers to dig into your email for some useful information. If your home address is public on Facebook, they can still track your home.

Most things that happen in our local homes are also part of the information on social media.

To protect how Facebook shows your information to people on its platform, you have to restrict certain personal details to only your Friends and private. We have categorized what and what to be shown to friends only and private (not visible to anyone except you)

What to be shared to Facebook public friends

- Your personal uploads
- Relationship status
- Workplace
- Town

What not to be shared to anybody

- Your Facebook friends
- Your phone number
- Your address unless if your Facebook account is a personal account
- Current city
- Family members

You can customize the list to your own preference.

To start personalizing the above information,

1. Go to your profile
2. Click **ABOUT**

From About page, edit the privacy to either Friends or Only me depending on how you choose your profile to be seen. Having done this, you have reduced the chance of your private information been stolen from untrusted people.

Facebook Anti-Social Engineering

Social engineering is a smart practice scammers use to manipulate a user (most especially on social media) into giving them access to something or providing sensitive information to them. The idea is to get something from who they are playing on.

They are expert in what they do – social engineers. They exploit one's weakness to offering them access to sensitive information. They can come as a corporate body or Facebook pages.

Assuming that your position at your workplace is an Accountant, they may pose as the company's Technical service asking some security details to update its server.

Here are some eye opener;

- When a stranger (someone you have not met) starts asking about your family, workplace and your position.
- When strangers forward websites that are too good to be true with some amazing offers. It could be a survey requiring only your name, email, zip code and physical address in case you win.
- When a profile of your family or close friend asks you for money or some unusual questions.

It is not that good no longer exist on Facebook and internet but one has to take a second thought about anything.

Futuristic and Advanced Facebook security

Why would someone be interested in manipulating over one's Facebook account in the first place? Facebook has become a crucial part of major businesses, networking, community and of course, friendly conversations.

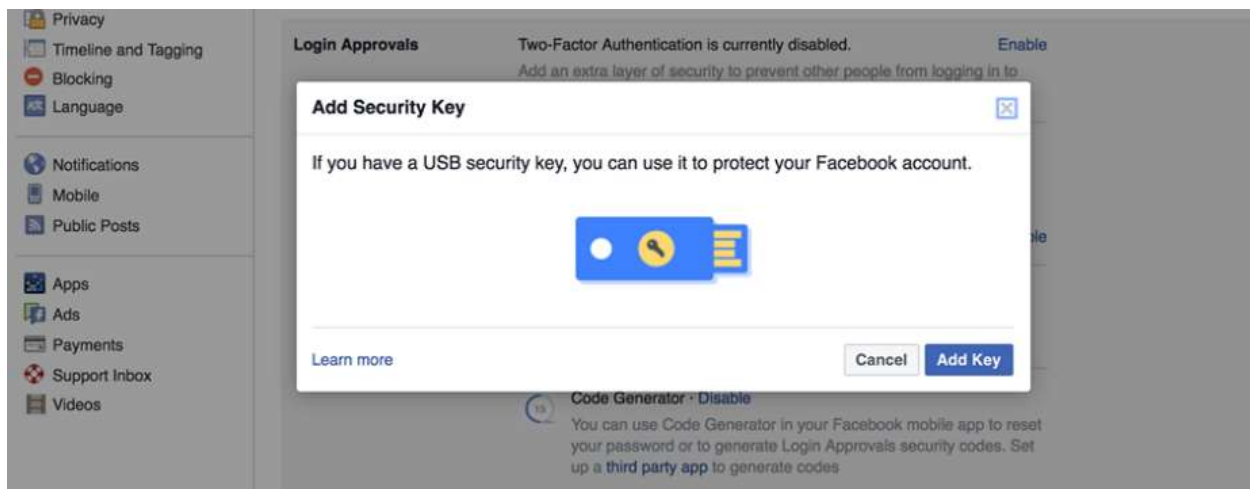
As such, when someone hacks into someone else Facebook account, they would be in a greater privilege to seeing who and what their victims are up to.

It is a big challenge to fight against this sort of social media discrimination. Facebook, with the above techniques you have read so far, has kept adding great tools to making Facebook a safer place for their users to entrust their personal information and credit cards for people using Facebook for business.

To further add extra protection to one's account, Facebook has improved on its security to advanced tools. They are;

- Security Key
- ThreatExchange program

Security Key



It is a portable USB stick just like that of a flash drive that you plug in into your computer (PC or MAC) and mobile phone (using NFC connectivity and Google Authenticator app) to grant login approval. Using login approval with Security Key can protect one's Facebook account from unauthorized access.

Security Key is an additional extension of two-factor authentication (text message, recovery codes and code generator) as we discussed in the previous sections but the idea of Security Key might be a better alternative to other options in two-factor authentication.

As Security Key being a hardware just like that of a token generator, one has to purchase it from recommended store, then registers it before use. After you have registered your Security Key, you would only be required to tap on the USB while it is plugged into your device to grant login approval.

Using security keys for two-factor authentication provides a number of important benefits:

- **Phishing protection:** Your login is practically immune to phishing (hacking attack) because you don't have to enter a code yourself and the hardware provides cryptographic proof that it's in your machine.
- **Fast login:** If you use a security key with your desktop computer, logging in is as simple as a tap on the key after you enter your password.

Security keys for Facebook logins currently only work with certain web browsers and mobile devices. It is also recommended to include other Facebook login approval method, such as text message or Code Generator.

To add a security key from your computer, you'll need to be using the latest version of Chrome or Opera. At this time Facebook has no support for security key logins for mobile Facebook app, but if you have an NFC-capable Android device with the latest version of Chrome and Google Authenticator installed, you can use an NFC-capable key to log in from Facebook mobile website.

Security keys can be purchased through [Yubico](#).

ThreatExchange

ThreatExchange is a project by Facebook to allow participants to share security threats on Facebook. Facebook created the ThreatExchange platform so that participating organizations can share threat data using a convenient, structured, and easy-to-use API that provides privacy controls to enable sharing with only desired groups.

ThreatExchange is a useful tool for businesses and corporate body on Facebook. To get started with ThreatExchange, you have to apply for a beta version. Click here to apply for [ThreatExchange](#).

If you are just a regular Facebook user, then this tool is not for you. It is for businesses on Facebook. Having read our previous pages on Facebook security and privacy, we believe that your future experiences on Facebook would be a great one.

Summary

Having gone through these security features to safeguarding one's Facebook account, we would also like to share a basic ground for you in case you are not certain on which option to adopt.

The main key thing to note is “How strong is your password”. Password is like a padlock to a house. If your padlock is old fashioned, cheap or not strong enough to resist tensional force on it, then it would be easier for burglarious folks to break in. So, form the habit of creating stronger password that you can't remember. Store your passwords in a place that it would be accessible anytime and anywhere.

The second thing to do is to define your login activity – how you would intend to login on Facebook. There are plenty of options to choose from including two factor authentication system (f2f). The recommended login system to choose are text message, code generator or get alerts when someone logs into your account.

The next step becomes controlling your activities and how your information are shared on Facebook. Restricting who sees what you share on Facebook strictly to a specific list of Facebook friends is a great choice. Sensitive information like personal details about family member, home address, place of works are to be shared with friends you trust.

Be smart when you engage with people on Facebook especially those people you haven't met. Be active enough to always review what happens on your timeline. You should also be careful with the types of Facebook applications we give access to our Facebook information.

At the moment you give access to apps on Facebook to tell you the number of kids to have, you have totally submitted your details to them. Nobody really knows if they are to stick to the privacy of not sharing your information to companies.

Do not be quick act on Facebook especially when it involves family and friends because you might be chatting with a total stranger who just hacked their account. When it involves information about your family, personal life then make sure to confirm in real life.

If it is about your work, also make sure to verify from the boss to avoid losing your job as a result of carelessness. The best step to take is [report to Facebook](#) and block. Tell your friends about it.

Last but not the least, be mindful on how you comment on posts on Pages, Groups and even friends. People who try to post what is irrelevant to the actual flag might be flagged by the other commenters as an automated account.

People do this with the view to entertain other people following the post but it is a bad practice. Don't spam Pages, Groups with links, they can report you to Facebook.

When one has a considerable spam reports from different people, Facebook may not take it lightly.

It is recommendable to frequently scan your Facebook account at least once in every 4 weeks using Facebook Security Checkup. Click [here to start security checkup review](#).

Resources:

1. ScamWatch <https://www.scamwatch.gov.au/report-a-scam>
2. BBB, A Better Business Bureau Study on How Scammers Use Impersonation, Blackmail and Trickery to Steal from Unsuspecting Daters
3. BBC <http://www.bbc.com/news/technology-43656746>
4. Facebook Security Page

Thank you for your time.

We would love to hear from you in order to assert the value of our material.

Send us a mail at book@chuksguide.com

If you also love to receive similar security updates as a bonus, sign up to our newsletter using the link below.

Stay safe!

With love from
James & Chuks