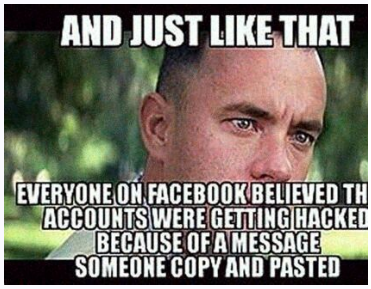
Fake facebook friend request generator

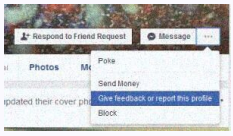
Click here for a summary of this article. Summary: Facebook Scams and How to Avoid Them Facebook is the most popular social media app in the world, and scammers flock to it to fleece unsuspecting users. So, to ensure you are aware of the most common Facebook scams we did some extensive research and found some of the most common tactics scammers employ. Here are the top 10 Facebook scams based on our research: Phishing: Emails or direct messages with sketchy links that download malware or capture login credentials on spoofed websites Romance: Friend requests and direct messages that attempt to create a romantic interest with the goal to steal money from the victim Prizes: Claims designed to obtain personal information or money from the victim Unrealistic job offers: Promises of dream jobs with little effort, in exchange for a user's personal information Shopping: Sales of counterfeit goods under a faux brand account Charity pleas: Fake charities to get donations during times of disaster Quizzes and games: Designed to elicit personal information in the answers, then hacking accounts with it Friend requests: Either from people you don't know or people you're already friends with (cloned accounts) Suspicious links about you: Messages that claim to contain impressive or embarrassing videos about you that usually contain malware Coupons and discounts: Apps that claim to get you discounts and coupons, but will only install malware on your device To protect yourself from scams on Facebook, always be skeptical of the messages, notifications, and links you receive. Don't click on anything you don't recognize, and don't share your personal information with anyone. On top of that, you can install Norton 360, the best antivirus to protect yourself from malware. You should also consider NordVPN, the best VPN to hide your personal information online and keep it away from hackers. Read on to learn more about how these Facebook scams work, and things you can do right now to avoid becoming a victim. Facebook is the world's most popular social media platform. Each month, more than 2.8 billion users log in to catch up with friends, share information, get their news, and even shop. But, the site's popularity makes it ripe for cybercriminals and all sorts of Facebook scams. So, how can you avoid becoming a victim of scams on Facebook? It starts by knowing what the most common scams are and the steps you can take to avoid them, which is what we'll be discussing in this article. Want to take the first step toward your online safety? We recommend getting NordVPN. This top VPN provider will help you hide your identity online and protect you from malware that is a prominent threat in Facebook scams. NordVPN's robust Threat Protection feature stops malicious software in its tracks. Try it now and get a great discount! Cybercriminals are an innovative bunch. They are always coming up with new ways to steal from unsuspecting social media users. Fraudsters most often try to get their hands on your account login credentials, personally identifying information, or bank and credit card information. They attempt this in a variety of ways through phishing emails, romance scams, Facebook quizzes, and more. Here's a complete Facebook scammer list: Facebook scams involving fake emails have been around for years, and Facebook users are not immune from receiving them.

Each month, more than 2.8 billion users log in to catch up with friends, share information, get their news, and even shop. But, the site's popularity makes it ripe for cybercriminals and all sorts of Facebook scams.

Each month, more than 2.8 billion users log in to catch up with friends, share information, get their news, and even shop. But, the site's popularity makes it ripe for cybercriminals and all sorts of Facebook scams. So, how can you avoid becoming a victim of scams on Facebook? It starts by knowing what the most common scams are and the steps you can take to avoid them, which is what we'll be discussing in this article. Want to take the first step toward your online safety?



Don’t click on anything you don’t recognize, and don’t share your personal information with anyone. On top of that, you can install Norton 360, the best antivirus to protect yourself from malware. You should also consider NordVPN, the best VPN to hide your personal information online and keep it away from hackers. Read on to learn more about how these Facebook scams work, and things you can do right now to avoid becoming a victim. Facebook is the world’s most popular social media platform.



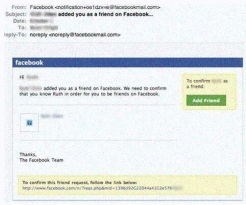
Here are the top 10 Facebook scams based on our research: Phishing: Emails or direct messages with sketchy links that download malware or capture login credentials on spoofed websites Romance: Friend requests and direct messages that attempt to create a romantic interest with the goal to steal money from the victim Prizes: Claims designed to obtain personal information or money from the victim Unrealistic job offers: Promises of dream jobs with little effort, in exchange for a user’s personal information Shopping: Sales of counterfeit goods under a faux brand account Charity pleas: Fake charities to get donations during times of disaster Quizzes and games: Designed to elicit personal information in the answers, then hacking accounts with it Friend requests: Either from people you don’t know or people you’re already friends with (cloned accounts) Suspicious links about you: Messages that claim to contain impressive or embarrassing videos about you that usually contain malware Coupons and discounts: Apps that claim to get you discounts and coupons, but will only install malware on your device To protect yourself from scams on Facebook, always be skeptical of the messages, notifications, and links you receive. Don’t click on anything you don’t recognize, and don’t share your personal information with anyone. On top of that, you can install Norton 360, the best antivirus to protect yourself from malware. You should also consider NordVPN, the best VPN to hide your personal information online and keep it away from hackers. Read on to learn more about how these Facebook scams work, and things you can do right now to avoid becoming a victim. Facebook is the world’s most popular social media platform. Each month, more than 2.8 billion users log in to catch up with friends, share information, get their news, and even shop. But, the site’s popularity makes it ripe for cybercriminals and all sorts of Facebook scams. So, how can you avoid becoming a victim of scams on Facebook? It starts by knowing what the most common scams are and the steps you can take to avoid them, which is what we’ll be discussing in this article. Want to take the first step toward your online safety? We recommend getting NordVPN. This top VPN provider will help you hide your identity online and protect you from malware that is a prominent threat in Facebook scams. NordVPN’s robust Threat Protection feature stops malicious software in its tracks. Try it now and get a great discount! Cybercriminals are an innovative bunch. They are always coming up with new ways to steal from unsuspecting social media users. Fraudsters most often try to get their hands on your account login credentials, personally identifying information, or bank and credit card information. They attempt this in a variety of ways through phishing emails, romance scams, Facebook quizzes, and more. Here’s a complete Facebook scammer list: Facebook scams involving fake emails have been around for years, and Facebook users are not immune from receiving them. You might even see them in your Facebook DMs. Phishing emails will include a link and some wording that encourages you to follow the link to Facebook, except it isn’t the real Facebook, just a spoofed website. Sometimes, the message will say you have compromised accounts. Other times, it will ask you to validate your login information. One growing trend is to send you an email link to reset your Facebook account, claiming it has been disabled for security purposes. Whatever the reason, the goal is always the same: to get you to provide confidential information to cybercriminals. Unfortunately, if you fall for this common scam, cybercriminals have all the information they need to wreak havoc in your life.

Depending on the information you provide, they can take over your Facebook account and con your friends, pretending to be you. They might also be able to access and drain your bank account or use your credit card to rack up fraudulent purchases. How to keep yourself safe: Don’t click on links from people you don’t know. If someone claims to be representing Facebook and they’re saying that something went wrong with your account, log into Facebook directly and check your settings there. You can also try NordVPN’s malware protection that will scan any files you download and prevent you from accessing any websites that can infect your device with malware. One of the oldest Facebook scams involves fraudsters posing as love interests to target unsuspecting Facebook users. These faux romancers are people you’ve never heard of before. A romance scam is designed to play on your emotions and gain your trust, so they may use flattery to woo you or pretend they’ve gone through a traumatic breakup to gain your sympathy. This isn’t a short-term effort. Chats build up over the course of weeks and months before the con-man makes their pitch. But it always ends the same way, as they eventually ask you to send money. It’s one of the most popular uses of catfishing online. The scammer can use a variety of reasons to get your money. One of the most popular is for the “romantic interest” to purchase airline tickets and visas so they can come and meet you in person. Another popular tactic is to say they need help covering their daily living expenses until they can eventually join you. In all cases, the affection is not real. If you fall for their pleas, you’ll end up with an empty bank account and a romance that never was. How to keep yourself safe: Be wary of people trying to flirt with you online.

People rarely decide someone is the love of their life after just checking out their profile. Most importantly, don’t send any money to people you haven’t met in real life.

The excitement of winning a prize is hard to resist. The problem is that scammers know this and use that excitement against you. Sometimes, they pose as celebrities, and other times as big brands you trust. Lottery scams are also common. In all cases, the prize is irresistible. All you have to do to claim your prize is to send a small fee to cover shipping or other processing costs. In some cases, you don’t even have to do more than scan a QR code. The goal is to get you to divulge your personal information, online account credentials, and bank or credit card information. Once you do, you never hear from the scammer again, and your only prize is identity theft or an empty bank account. How to keep yourself safe: Don’t agree to cover any processing costs or advance fees for “prizes.” Be wary of people claiming you’ve won something when you haven’t participated in any contests or giveaways. The allure of a high-paying job opportunity might be hard to resist, especially when it comes without having to do anything yourself. But before you say yes to any unexpected offer, understand this is a common scam on Facebook used by cybercriminals to extract personally identifying information

from you. If you respond to an offer like this, you'll be asked to provide the typical information needed to start any job — your home address, your social security number, and perhaps even a copy of your driver's license or passport. Unfortunately, this is all a clever criminal needs to steal your identity. Instead of a job, you get a financial mess to clean up. How to keep yourself safe: Be wary of people claiming you got a dream job without even having to interview. Before submitting your personal information to places of employment, make sure it's a legitimate company.



Here are the top 10 Facebook scams based on our research: Phishing: Emails or direct messages with sketchy links that download malware or capture login credentials on spoofed websites Romance: Friend requests and direct messages that attempt to create a romantic interest with the goal to steal money from the victim Prizes: Claims designed to obtain personal information or money from the victim Unrealistic job offers: Promises of dream jobs with little effort, in exchange for a user's personal information Shopping: Sales of counterfeit goods under a faux brand account Charity pleas: Fake charities to get donations during times of disaster Quizzes and games: Designed to elicit personal information in the answers, then hacking accounts with it Friend requests: Either from people you don't know or people you're already friends with (cloned accounts) Suspicious links about you: Messages that claim to contain impressive or embarrassing videos about you that usually contain malware Coupons and discounts: Apps that claim to get you discounts and coupons, but will only install malware on your device To protect yourself from scams on Facebook, always be skeptical of the messages, notifications, and links you receive. Don't click on anything you don't recognize, and don't share your personal information with anyone.

On top of that, you can install Norton 360, the best antivirus to protect yourself from malware. You should also consider NordVPN, the best VPN to hide your personal information online and keep it away from hackers. Read on to learn more about how these Facebook scams work, and things you can do right now to avoid becoming a victim.

Facebook is the world's most popular social media platform. Each month, more than 2.8 billion users log in to catch up with friends, share information, get their news, and even shop. But, the site's popularity makes it ripe for cybercriminals and all sorts of Facebook scams. So, how can you avoid becoming a victim of scams on Facebook? It starts by knowing what the most common scams are and the steps you can take to avoid them, which is what we'll be discussing in this article. Want to take the first step toward your online safety? We recommend getting NordVPN. This top VPN provider will help you hide your identity online and protect you from malware that is a prominent threat in Facebook scams. NordVPN's robust Threat Protection feature stops malicious software in its tracks. Try it now and get a great discount! Cybercriminals are an innovative bunch. They are always coming up with new ways to steal from unsuspecting social media users. Fraudsters most often try to get their hands on your account login credentials, personally identifying information, or bank and credit card information. They attempt this in a variety of ways through phishing emails, romance scams, Facebook quizzes, and more.

Here's a complete Facebook scammer list: Facebook scams involving fake emails have been around for years, and Facebook users are not immune from receiving them. You might even see them in your Facebook DMs. Phishing emails will include a link and some wording that encourages you to follow the link to Facebook, except it isn't the real Facebook, just a spoofed website. Sometimes, the message will say you have compromised accounts. Other times, it will ask you to validate your login information. One growing trend is to send you an email link to reset your Facebook account, claiming it has been disabled for security purposes. Whatever the reason, the goal is always the same: to get you to provide confidential information to cybercriminals. Unfortunately, if you fall for this common scam, cybercriminals have all the information they need to wreak havoc in your life. Depending on the information you provide, they can take over your Facebook account and con your friends, pretending to be you. They might also be able to access and drain your bank account or use your credit card to rack up fraudulent purchases. How to keep yourself safe: Don't click on links from people you don't know. If someone claims to be representing Facebook and they're saying that something went wrong with your account, log into Facebook directly and check your settings there. You can also try NordVPN's malware protection that will scan any files you download and prevent you from accessing any websites that can infect your device with malware. One of the oldest Facebook scams involves fraudsters posing as love interests to target unsuspecting Facebook users. These faux romancers are people you've never heard of before. A romance scam is designed to play on your emotions and gain your trust, so they may use flattery to woo you or pretend they've gone through a traumatic breakup to gain your sympathy. This isn't a short-term effort. Chats build up over the course of weeks and months before the con-man makes their pitch. But it always ends the same way, as they eventually ask you to send money. It's one of the most popular uses of catfishing online. The scammer can use a variety of reasons to get your money. One of the most popular is for the "romantic interest" to purchase airline tickets and visas so they can come and meet you in person. Another popular tactic is to say they need help covering their daily living expenses until they can eventually join you. In all cases, the affection is not real. If you fall for their pleas, you'll end up with an empty bank account and a romance that never was. How to keep yourself safe: Be wary of people trying to flirt with you online. People rarely decide someone is the love of their life after just checking out their profile. Most importantly, don't send any money to people you haven't met in real life. The excitement of winning a prize is hard to resist. The problem is that scammers know this and use that excitement against you. Sometimes, they pose as celebrities, and other times as big brands you trust. Lottery scams are also common. In all cases, the prize is irresistible. All you have to do to claim your prize is to send a small fee to cover shipping or other processing costs.

In some cases, you don't even have to do more than scan a QR code. The goal is to get you to divulge your personal information, online account credentials, and bank or credit card information. Once you do, you never hear from the scammer again, and your only prize is identity theft or an empty bank account. How to keep yourself safe: Don't agree to cover any processing costs or advance fees for "prizes." Be wary of people claiming you've won something when you haven't participated in any contests or giveaways. The allure of a high-paying job opportunity might be hard to resist, especially when it comes without having to do anything yourself. But before you say yes to any unexpected offer, understand this is a common scam on Facebook used by cybercriminals to extract personally identifying information from you.

If you respond to an offer like this, you'll be asked to provide the typical information needed to start any job — your home address, your social security number, and perhaps even a copy of your driver's license or passport. Unfortunately, this is all a clever criminal needs to steal your identity. Instead of a job, you get a financial mess to clean up. How to keep yourself safe: Be wary of people claiming you got a dream job without even having to interview. Before submitting your personal information to places of employment, make sure it's a legitimate company. Facebook has grown from a simple social network app to a robust e-commerce platform. Businesses of all sizes maintain a page and regularly promote their goods and services via sponsored posts. Unfortunately, cybercriminals capitalize on the popularity of Facebook Marketplace, too, particularly with scam ads. Scammers create fake brand accounts to push counterfeit goods. Other times, they create unheard-of shop names with "too good to be true" offers, then push scam ads like the one below. These unknown sellers offer goods at ridiculously cheap prices but don't deliver anything at all. Instead, they take your money and disappear. Another common tactic in this Facebook scam is to claim that they're clearing out their inventory, and so you just need to cover shipping to get free items. Sometimes, you might even get the product. But it'll be a low-quality version, and the "shipping" cost you covered actually paid for the product and then some. How to keep yourself safe: If a product's free, and you

only need to cover the shipping, you'll probably never see the goods. Don't pay for allegedly "free" items from unknown brands. When disaster strikes, it is human nature to want to help. For many, this means donating money.

Fraudsters know this and use crises to reap a quick payday through a Facebook scam. They create fake charity pages, websites, and even accounts on popular sites like GoFundMe, then promote their "charities" on your Facebook feed. Fake charity scams are usually connected to PayPal scams, as the fraudsters ask you to pay via a PayPal account. How to keep yourself safe: Before you give a dime to any charity, do a little research. There are sites specifically designed to help you identify legitimate charities, like Charity Navigator, Guidestar, and Charity Watch.

All those "getting to know you better" and "just for fun" quizzes you see on Facebook seem innocent enough. But these Facebook scams are anything but innocent. They are all designed to extract the kind of personal information many people use to create passwords or answer security questions for their online accounts. Cybercriminals know this and use these quizzes to hack into a user's Facebook account. From there, they can do a lot of damage beyond simply taking over your Facebook account. How to keep yourself safe: Don't fill out fun Facebook quizzes and games with your personal information. Anyone who's been on Facebook for a while has encountered this scam. You get a Facebook friend request from someone you swear you are already friends with. This is a favorite tactic by scammers, who replicate entire Facebook accounts to mimic a legitimate person. When you accept a fake request, you give the scammer insider access to you, even if you have your Facebook account locked down. They may even engage with you and use your trust to coax you into falling for their other scams, like a bogus link that installs malicious software on your device. How to keep yourself safe: Ignore friend requests from people you already have on your list, at least until you can confirm it's them sending the request and not a Facebook scam. Anyone on Facebook knows the sinking feeling in the pit of your stomach when you open a Facebook private message that claims to have a video of you.

These messages come from one of your Facebook connections and say something like "OMG! Is this you?" or "Have you seen this yet?!" In reality, it isn't your friend who sent the message. Their account got hacked, and it is a fraudster using your friend's account (or a cloned account mimicking your friend's) to send malware links. The purpose of this scam on Facebook? To get you to click on the video or link. Once you do, you'll usually be redirected to a website that installs malware on your device. Once it infects your computer, tablet, or smartphone, scammers have control and can spread malware to your friends and family. How to keep yourself safe: Don't click on any random links from people, especially if they claim to have videos of you. If you do click on the video, you don't even need to install anything for your personal information to be in danger. If you just access the site, its owner can get your IP address, which they can then use to wreak more havoc on your online life. Make sure you protect your personal information with a VPN like NordVPN, which will hide your IP address. Another tried-and-true Facebook scam is playing to the allure of saving money. Hackers push these great deals to unsuspecting victims in a variety of ways.

One of the most popular is through bogus apps that promise great deals on online shopping. This happens with alarming frequency and is highly effective. Unfortunately, the app is really a Trojan horse. When the user installs it on their phone or computer to claim their coupons or discounts, what they're actually getting is malware. Once installed on your device, the malware can do many things, like extract confidential information and send it on to cybercriminals. But you won't get any discounts or coupons. How to keep yourself safe: Only install apps from your phone's official store. Even then, only install apps from reputable developers. On computers, don't install any apps that claim to give you discounts. Legitimate coupon apps can work just fine in your browser, and they don't need to be on your system. Another Facebook scam similar to the "You Won!" scheme is the giveaway scam. With this one, fake pages will usually claim they're giving away a ludicrous amount of free iPhones or gaming consoles.

All you have to do to join the giveaway is give your personal details to the page, or worse, go to an external website and fill out a form there. But there's no giveaway, and your personal data will be stolen. Real giveaways don't need your personal information and will usually just ask you to leave a random comment and follow their page on Facebook. How to keep yourself safe: Don't join any giveaways unless you know and trust the organizing page. Even then, don't submit any personal details like your legal name, password, or email. This one is more common on Instagram, but we have seen cases of such a scam on Facebook as well. You'll see apps that promise to notify you if someone unfriends you, unfollows you, or unlikes your page. Sometimes, these apps might promise other attractive deals for page owners, like free likes, follows and interactions with your profile. Even if these apps live up to the promises, they most likely can't provide you with the audience you're looking for. But generally, you'll just submit your data to these apps and get nothing in return. How to keep yourself safe: Don't install any apps that promise attractive functionalities for Facebook. Don't provide your login credentials or any other sensitive information to third-party apps. If you've ever managed a Facebook page, you'll know that its messages show up as notifications in your personal Facebook profile. Cybercriminals use this Facebook scam to try and trick people into thinking they got a notification from Facebook. (The original message in Spanish reads: "Your page has been restricted because it does not comply with our Community Standards. We know that we are not always right.

As such, if you think we have made an error, you can confirm your identity and appeal this decision. According to the Community Standards of Facebook, you have 24 hours to follow these steps to avoid your account's permanent deactivation. Confirm your identity: (malicious link) Thanks!") They'll send a message from a page like "Facebook Security Monitor" claiming your account was breached, your payment has failed, or anything that requires immediate attention.

You just need to click on their link to solve the problem. If you do, you may inadvertently install malware like a computer virus on your PC or even fall for a spoofed version of Facebook that steals your login credentials. How to keep yourself safe: Don't click on any links from unknown sources. If you get a notification about your page's security, but it's actually a message in your page's inbox, ignore it and report the sender to Facebook. Moreover, to enhance your online protection and protect your device from malware, we recommend getting NordVPN. Any link you click on will be scanned with NordVPN's malware protection software, instantly blocking any harmful programs from infecting your device. Like loan scams anywhere on the web, this scam on Facebook involves people sending messages or posting about instant loans with low-interest rates.

All you have to do is send a small advance or processing fee.

Of course, if you do make the payment, you'll never see the loan. Depending on what forms you fill out, your personal data might also be in danger.

How to keep yourself safe: If you need a loan, make sure you only apply to licensed financial services providers. If an interest rate sounds too low to be true, it's probably a scam. When hackers manage to breach a big Facebook account, they may broadcast a pre-recorded message live. This message will usually feature a call to action, such as an investment opportunity or a link to another site that will attempt to steal your data. Since people assume it's a recommendation from their favorite creator, many of them will actually go through with the call to action. If it's an investment opportunity or a product on the other side of the link, the users will never see their money again. Alternatively, you may just be sent to a site that steals your data or tries to install malware on your device. How to keep yourself safe: If your favorite influencer is live, make sure it's actually them behind the screen. If they make uncharacteristic recommendations or broadcast unusual ads, be very skeptical and don't click on any links, as it may very well be a Facebook scam. The holiday spirit is beautiful, and organizing a Secret Santa with your coworkers is always fun. But be very reticent when you get the same offer over Facebook. Scammers will pretend they're organizing a massive Secret Santa worldwide, and all you have to do is send this random person a gift card or some such low-value gift. In exchange, you're promised dozens of gifts from other jolly fellows like yourself. Of course, this "random" person is none other than the scammer. Like most Ponzi schemes, the first few people who join may actually receive a gift to build credibility. But most people won't see anything in return for their gift, all while the scammer is raking in dozens of free gift cards and wine bottles. How to keep yourself safe: Don't join Secret Santa games with people you don't know. You may find legitimate surveys on Facebook. But beware, since scams designed to steal your data can be disguised as surveys. These will usually make outlandish promises, such as free iPhones, to all participants who just fill out a survey. In most cases, you'll also have to share a link to the survey before being allowed to participate. In reality, all the data you submit through the survey is collected by hackers and then used for identity fraud. How to keep yourself safe: Don't fill out surveys that make unrealistic promises, ask you to share them, or ask for too much personal information. If you do fill out surveys, make sure the website you're on is a reputable survey provider to protect yourself from identity theft. There are many things you can do to maintain your safety and avoid becoming a victim

in any of the ways we have outlined in our Facebook scammer list above. From within Facebook, follow these best practices to avoid fraudsters. To avoid attracting unwanted attention from cybercriminals, be sure your account is as private as possible. While you can never hide your profile pictures or cover photos, you can hide almost everything else from those outside your friend's list. You can also tweak your Facebook privacy settings in other ways to keep your account safe. Here is how to do so from your computer: Open the Facebook app. Click on the down arrow (on iPhone) or hamburger menu (on Android) in the upper right corner of the screen. Choose "Settings & Privacy" from the menu. On iPhone, select "Privacy Checkup." On Android, click "Settings," which will lead you to another page where "Privacy Checkup" is. Facebook will walk you through the most common privacy settings, with recommendations for each option. One of the easiest ways to prevent unwanted logins on your Facebook account is to enable two-factor authentication. With this in place, anytime someone tries logging in from an unrecognized location or device, they will also have to enter a one-time code in addition to their username and password. This code is sent to your phone via text or an authenticator app. To set up two-factor authentication on Facebook, do the following: Open the Facebook app on your computer. Click on the down arrow in the upper right corner of the screen.

Choose Settings & Privacy > Settings > Security & Login. Scroll down to Two-Factor Authentication and click Edit. You'll be able to set up a secondary method of authentication based on your preferences. This is an easy one. Get in the habit of declining friend requests from anyone you are not familiar with. Unless you are trying to become a Facebook influencer, amassing connections with people you don't know is unnecessary and unsafe. The more friends you have that you don't know, the higher the risk you'll be approached with some sort of Facebook scam. If you receive a private message from someone you know and they're pleading for help (usually in the form of money), double-check with this friend off Facebook to verify the legitimacy of their request. Logically, if a real friend is in dire straights, they won't rely on Facebook Messenger to get help. Use WhatsApp (or another messaging service) to reach out to them. Go old school and call them. However you do it, take this extra step to prevent being scammed. Most likely (always?), Facebook Messenger requests for help are a simple scam to extract money from you. Whether it is a phishing email or a private message from a friend, avoid the temptation to click on unsolicited videos or links. If you think a friend sent you something, double-check with them (outside of Facebook) before clicking on anything. Especially when what they sent you involves embarrassing or compromising information about you. Most real friends would probably not send a generic "OMG! Is this you?!" message if they really saw something bad about you. Facebook may occasionally send you an email that contains links. If you want to verify that the email is legitimate, you can check it by following these steps: Open the Facebook app on your computer. Click on the down arrow in the upper right corner of the screen.

Choose Settings & Privacy > Settings > Security & Login. Scroll down to "Advanced" and click "Recent Emails from Facebook." Here, you will find all the real emails Facebook has recently sent you, both about security and login issues, as well as other topics.

If the email is listed here, you can be confident it's the real deal and not a scam on Facebook. Be sure to keep an eye on all the places and devices that are logged into your Facebook account. This helps you get rid of unwanted access quickly. Here's how to check your log-in sessions: Open the Facebook app on your computer. Click on the down arrow in the upper right corner of the screen. Choose Settings & Privacy > Settings > Security & Login.

Scroll down to "Where You're Logged In" and review for accuracy. Delete any suspicious logins.

Resist the urge to reuse passwords across multiple online accounts. Also, make sure the unique password you use is hard to decipher. The days of using your oldest child's birthday or mother's maiden name are long gone. Today's sophisticated cybercriminals can crack most simple passwords with ease. Whether you use the password manager included in your browser, enlist the help of a third-party app, or create your own complex passwords (and save them somewhere very secure), your online security is greatly improved when you use strong passwords. If you don't want to bother remembering all of these passwords, we recommend NordPass. It's the best password manager out right now, and we've used it without a worry. If you want alternatives to NordPass, check out our roundup of the best password managers. If you are one of the millions of people who shop on Facebook, keep yourself safe by only dealing with verified Facebook pages. This extra step is taken by all reputable brands to reassure potential buyers of the integrity of any transaction.

It is easy to see which brands are verified. They will have a blue circle with a checkmark next to their brand name. If a Facebook page is selling items but not verified, think really hard before providing personal information or credit card details to them, as it may very well be a Facebook scam. To avoid the damage of someone cloning your Facebook account and using these fake accounts in malicious ways, get in the habit of regularly searching Facebook for your name. This only takes a minute and is an easy way to identify and eliminate doppelganger accounts. If you do find an imposter account, you can report it to Facebook by using the Report Profile feature. Just click on the three dots on a person's profile and select Find Support or Report Profile. There are several things you can do to ensure your safety on Facebook and online in general. Developers regularly issue patches to deal with security issues as they become known. If you are not in the habit of regularly updating your operating system, your device is unnecessarily vulnerable. Update your devices anytime a new release is issued. You can turn on auto-updates to automate the process. If you think an email you received from Facebook is a scam, go ahead and forward it to Facebook. They will take it from there. The official email to send it to is phish@facebook.com. To avoid the possibility of malicious software being installed on your devices, make sure to have a robust antivirus program installed and running on your smartphone, computers, and tablets.

If you want malware protection right now, we recommend Norton 360. We tested all the popular antivirus apps, and we analyzed reports from independent testers like AV-Comparatives. From our research, we can confidently recommend Norton 360 to anyone trying to protect their device from malware. Avoiding Facebook scams involves using simple common sense. An offer that seems too good to be true? It probably is. That video link your friend sent you with the "Is this you!?" comment? Likely fake. The friend request with a suggestive message from someone you don't know? It was probably the start of an eventual money request. The bottom line is to be skeptical and vigilant whenever you interact on Facebook. Only accept friend requests from people you know in real life.

Pass on those incredible offers sent out of the blue. Don't overshare or give out personal data. If you inadvertently click on a malicious link, the site's owner can see your IP address, which may reveal your location, ISP, and plenty more personal information.

A VPN (virtual private network) is another layer of protection against cybercriminals because it hides your IP address. So when you're connected to a VPN, crucial personal data is hidden from prying eyes.

Plus, if you get a trusty VPN like NordVPN, you also get an ad blocker and protection from malware. We tested all the popular VPNs, and we're happy to recommend NordVPN, thanks to its fast speeds, airtight security, and great price. If you use our exclusive link, you can also get 69% off your subscription. Even the most vigilant Facebook user might fall victim to a cleverly crafted Facebook scam, like the ones we discussed in our Facebook scammer list.

There are many ways cybercriminals can hurt you, including: Infecting your devices and spreading malware to your contacts Racking up credit card charges Draining your bank account Ruining your credit Stealing your identity As soon as you think you've been a scam victim, you must move quickly to minimize the damage. Here are some things you should do right away to protect yourself: If you believe your Facebook account has been hacked, change your password immediately. If you've used this password on other accounts, be sure to change it there, too. Whenever your login credentials fall into the hands of cybercriminals, you should also consider changing passwords on all your sensitive accounts, including your bank and credit card companies. Make sure the new passwords are secure by being unique and complex. It only takes a second to report questionable profiles, ads, posts, or messages to Facebook.

You will find a Report option on every page, post, and direct message. However, not all scammers get their accounts suspended — and even if they do, they can always attempt to get unbanned on Facebook. Unfortunately, Facebook has been under fire over the past few years for consistently failing to meet users' expectations on moderation and regarding Facebook scams. Reports go ignored, and blatant breaches of the Community Standard are left unaddressed. We've even had disgruntled Facebook users comment under this post, mentioning the company's inability to moderate scams properly. So, what can you do if Facebook doesn't take your report seriously? Unfortunately, there's no guarantee they will ever take the right measures. But here are a few things you can try: Get your friends and acquaintances to report as well. We've seen this work, especially for fake accounts. When something is reported en masse, there's a higher chance Facebook will take it down or at least have a human moderator look at it. Get in touch with Facebook over one

of their official points of contact. They have a dedicated form to appeal moderation decisions. Appeal the moderation decision. You can do this by providing more context, such as proof of identity or anything that can persuade Facebook to take action. You should get in the habit of regularly monitoring all the accounts where you have money or credit lines. Cybercriminals often initiate smaller transactions to test for success before they go in for the kill during a scam on Facebook. By identifying suspicious transactions early, you can prevent major damage to your finances and credit. If you think your personal information has fallen into the wrong hands and are concerned about identity theft, be sure to freeze your credit. If you don't, scammers can do many things, like open bank and credit card accounts in your name, obtain utility and cell service, and even apply for mortgages all in your name. This can have devastating effects on your creditworthiness. You can prevent this by freezing your credit at the major credit reporting agencies. When you do, no new credit will be issued under your social security number or name. In the United States, you can do this at Experian, TransUnion, and Equifax. The United Kingdom and most European countries offer similar services for their respective jurisdictions. If thieves infiltrated your Facebook account or installed malware on your device, it is possible they have all the information they need to steal your identity. But you may not catch it early enough to prevent serious damage.

To avoid that, many people turn to identity theft monitoring services. One such company is LifeLock. They'll help you monitor your data and take swift action in case of a breach. You can head directly to their website to find out more or check out our Lifelock review. Facebook is a great way to keep up with friends and family.

It's also a convenient place to follow your favorite celebrities, brands, and news outlets. But the social media channel doesn't come without risks, including numerous Facebook scams. To stay safe while you scroll, like, share, and comment, you must remain vigilant. Know the most popular types of scams on Facebook, cast a wary eye on private messages you receive, don't accept friend requests or messages from strangers, and never send money to people you don't trust. It is essential also to maintain safe online habits and run antivirus software on all your devices. For an added layer of security, don't forget to also use NordVPN to hide your IP address and protect your personal data. These sensible strategies will keep you safe on Facebook and many other social media platforms. Learn more about other social media scams and how to avoid them here: 17 Facebook Scams and How to Avoid Them: Frequenty Asked Questions Didn't find what you were looking for in our article?

Still have questions? Check out the questions we get asked most often about Facebook scams. How do I report a Facebook scam? Facebook makes it easy to report a suspected scam post, account, page, or direct message. There is always a Report option available on every Facebook screen.

To access it, you'll most often need to click on the three dots next to a profile name, message, or post. Just click on the Report option, follow any additional prompts, and Facebook will investigate your scam claim. What are the most common Facebook scams? Phishing emails and romance attempts are two of the most common scams involving Facebook. Phishing tries to get you to click on sketchy links that want your private information or attempt to install malware on your device. Faux romancers try to hook you and convince you to send them money. What should I do if I fall for a Facebook scam? If you think you are a Facebook scam victim, the first thing you should do is change your login credentials. If you used the same password elsewhere, change it there, too. Also, report the scam to Facebook. You should also keep close watch on your financial accounts for any suspicious activity. Depending on the type of information you disclosed, you may also consider freezing your credit and subscribing to an identity theft monitoring service like LifeLock.

Theodor is a content writer passionate about the newest tech developments and content marketing strategies. He likes privacy-friendly software, SEO tools, and when he's not writing, he's trying to convince people they should uninstall TikTok.