

10 critical steps to help protect yourself online

You've heard these recommendations ??? How many times!!

We re going to review them again and add a few for this group.

You can help protect yourself online by using strong passwords, avoiding dangerous links, backing up your data, and more. Here are our 10 most important tips for staying safe online.

1. Don't open mail from strangers

- Even if it looks interesting Do no open the e-mail!
- If you get a phishing email with malware attached, you don't have to download the attachment for it to do damage to your home network. That's because drive-by downloads can install malware on your hard drive without you even agreeing to download them.

In some cases, a drive-by download might disguise itself as a standard system update or another innocuous “yes / no” question, and even the most cyber-savvy among us can be fooled. **For this reason, it's a good idea to refrain from opening any emails from addresses you don't know.**



2. Make sure your devices are up to date

- You have heard this at least 1000 times!!
- If you don't have your security software, web browsers, and devices set to update automatically, [turn on those automatic updates](#) now. Updates often include critical fixes for any security holes that may have been detected in your programs or devices.
- Updates can be time consuming but YOU can control when they take place

3. Use strong passwords

- There are several ways to protect yourself from identity theft online, and using strong passwords is one of them. Unfortunately, even now, people still use passwords like “12345678” or “password.” Don’t use those, and also don’t use your dog’s name or your kids’ birthdays.
- *The best password is one that you can remember*, but one that will be hard for other people, even malicious programs that try every password combination under the sun, to guess.
- An abbreviated sentence, or passphrase, is often better than a single word with numbers and symbols inserted. Or
- You can use a password management app to generate and store your passwords for you. A password manager can also help you generate unique passwords for each of your online accounts.
- For extra security, change your passwords several times per year.

4. Use two-factor authentication

- At the very least use this for your most sensitive apps
- Two-factor authentication requires you to verify your identity after you've logged in using your username and password.
- In some cases, you'll be asked to verify your identity by entering a code sent by text to your phone or by email.
- Other times, you'll have to answer a security question. *(Don't forget the answers to the questions)*.
- Whenever two-factor authentication is available, opt in. It may take you a couple of extra seconds to log in to your accounts, but it can make it less likely that other people will be able to log into your accounts, too.



5. Don't click on strange-looking links

- Viruses and other forms of malware often spread because you click on a link from someone you know.
- If you receive a link that looks strange (for instance, it may have typos in it) from a trusted friend or family member, contact them to ask if the link you've received was sent on purpose.
- You might have to wait a bit to watch that funny viral video, but better safe than sorry.
- If you don't want to wait for a response from your friend or family member, copy and paste the link into a reputable link checker. But remember: Don't click on the link.

7. Back up your data regularly

- If you become a victim of malware, such as ransomware, you might not be able to get your data back. That is, unless you've backed up your data.
- When you back up your data, you can make certain kinds of security breaches less problematic. If a hacker encrypts your data and demands a ransom to unencrypt it, it's not going to be that big of a deal if you backed it up a week ago.

8. Be smart with financial information

- Be mindful of where you enter information like your credit card number online.
- Before you purchase anything on a website, ensure that the website's URL starts with "https://." The "s" at the end is critical, because it indicates that your connection is encrypted.
- Or has the LOCKED symbol  the in the URL
- Don't purchase anything from  bsite that doesn't have this.
- You should think twice about saving your financial information to websites you buy from, even if you shop with them frequently.
- Storing your information on their site could make it easier for hackers to access in the event that company's website or network suffers a data breach.

9. Educate your family

- You can be taking all the right precautions on your home security network, but if your family and other people using your network aren't doing their part to keep everything secure, your efforts might not be enough.
- Make sure that everyone who regularly uses your network knows how to help keep it secure.

10. Avoid sharing personal information

- It's easy to get comfortable with sharing a little too much personal information online.
- You may be surprised at how much damage cybercriminals can do with just a little bit of information.
- To keep it safe, never share identifying details, like your full name, address, or financial information with strangers you meet online.
- You should also be careful about the usernames you create for websites — there's no need for them to include your real name.
- Be sparing with the amount of information you share in online surveys or forms. Most of the time, little to no personal information is genuinely needed to complete them.

10. Avoid sharing personal information Cont

- Staying safer online can feel like a challenge, but it doesn't have to be.
- If you're still learning how to protect yourself against online predators or scams, just treat interactions online the same way you would treat interactions with a stranger walking down the street.
- That is, you probably wouldn't open anything they give you, hand them your credit card, or lead them to your home address.
- The same rules can help you stay safer online.

Pop up message saying to call Microsoft Technical support for immediate help:

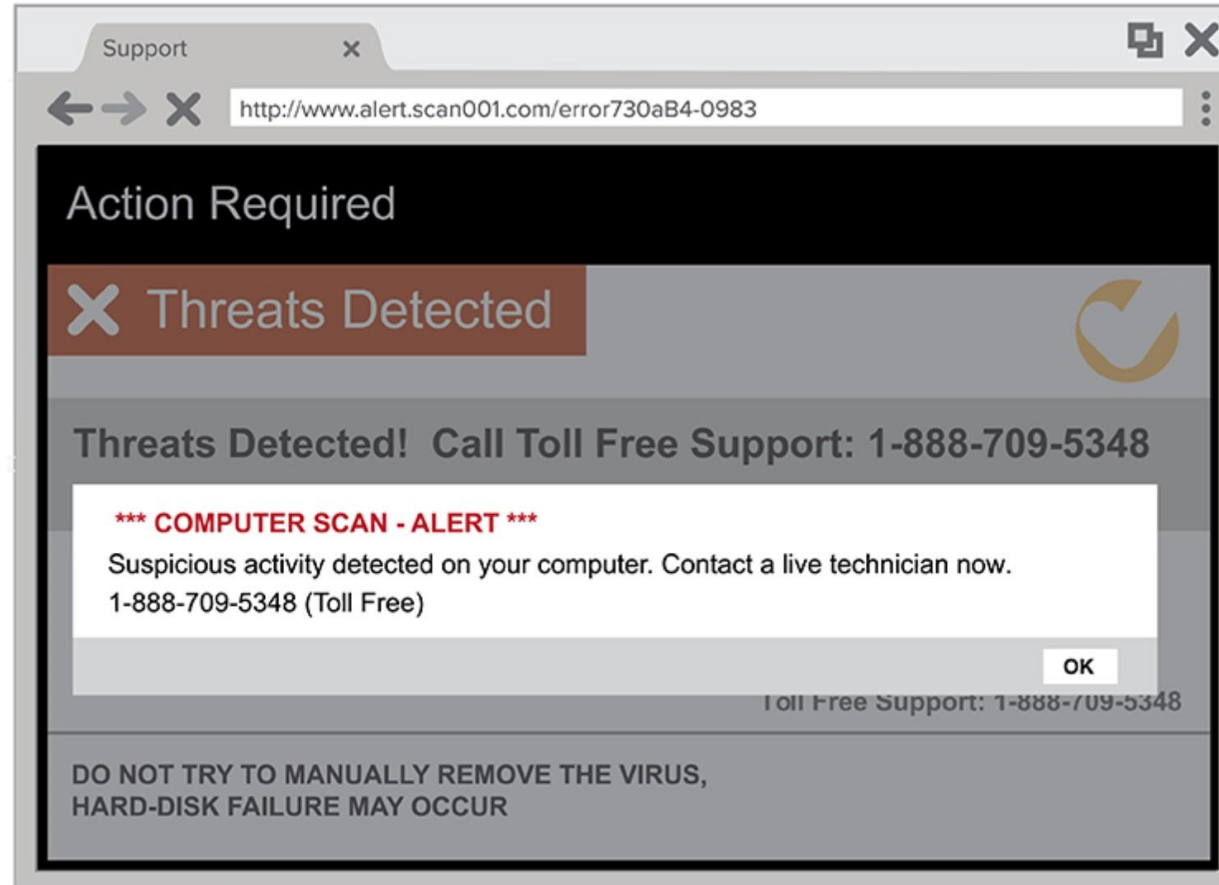
- Has anyone seen a pop up message saying the following:
- Windows detected suspicious activity on your Computer.
- Please contact Microsoft Technical support for immediate help:
- @ 800(toll free).
- Your Computer ID: and has a 5-digit number
- Please contact Technical support to resolve this issue.
- DO NOT open any additional internet browser to avoid data corruption on the registry of your operating system. Please contact Microsoft Support at
- Toll-free Helpline removed
- DO NOT SHUT DOWN OR RESTART THE COMPUTER. DOING SO MAY LEAD TO DATA LOSS AND POSSIBLE FAILURE OF
- Then it has an OK button to click.

“Apple Support” pop-up Virus scam



The **Official Apple Support pop-up scam** is a misleading advertising that was created in order to force you into calling a fake Apple Support Service.

Pop-up warnings



If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.

2 Things To Know To Avoid a Tech Support Scam

- 1. Legitimate tech companies won't contact you by phone, email or text message to tell you there's a problem with your computer.
- 2. Security pop-up warnings from real tech companies will never ask you to call a phone number.

What To Do if You Think There's a Problem With Your Computer

- If you think there may be a problem with your computer, [update your computer's security software](#) and run a scan.
- If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

What To Do if You Were Scammed

- If you paid a tech support scammer with a credit or debit card, you may be able to stop the transaction. Contact your credit card company or bank right away. Tell them what happened and ask if they can reverse the charges.
- If you paid a tech support scammer with a gift card, contact the [company that issued the card](#) right away. Tell them you paid a scammer with the gift card and ask if they can refund your money.
- If you gave a scammer remote access to your computer, [update your computer's security software](#). Then run a scan and delete anything it identifies as a problem.
- If you gave your user name and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a [new password that is strong](#).

Avoid Tech Support Refund Scams

- If someone calls to offer you a refund for tech support services you paid for, it's likely a [fake refund scam](#).
- How does the scam work?
- The caller will ask if you were happy with the services you got. If you say, "No," they'll offer you a refund.
- In another variation, the caller says the company is giving out refunds because it's going out of business. No matter their story, they're not giving refunds. They're trying to steal more of your money.
- Don't give them your bank account, credit card or other payment information.

The Number one Place for Phishing is FACEBOOK



Facebook Continued

- **Phishing scams:**
- Scams involving **fake emails** have been around for years, and Facebook users are not immune from receiving them.
- Phishing email 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.

Facebook Continued

- **Romance scams**

- One of the oldest scams involves fraudsters posing as love interests to target unsuspecting Facebook users. These faux romancers are people you've never heard of before.
- Scammers pretend they've gone through a traumatic breakup or use flattery to woo you.
- A romance scam is designed to **play on your emotions and gain your trust.**

Facebook Continued

- **You've won! scams**

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, other times as big brands you trust.

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](#).

Facebook Continued

- **Bogus job scams**

- The allure of a high-paying job opportunity might be hard to resist, especially when it comes without having to do anything yourself.
- Before you say yes to any unexpected offer, understand this is a common technique used by cybercriminals to **extract personally identifying information from you.**

Facebook Continued

- **Shopping scams**

- 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 shopping, too, particularly with scam ads.

Facebook Continued

- 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.

09:17



Sponsored · 🌐



🎁 Everything is FREE, just pay shipping! 🎁
Only at ✨ [Redacted]



[Redacted]
Women's Clothing Store

Shop Now



Write a comment...



Facebook Continued

- **Fake charity scams**
- 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. They **create fake charity pages, websites, and even accounts on popular sites like GoFundMe**, then promote their “charities” on your Facebook feed. Usually, they ask you to [pay via a PayPal account](#).
- Before you give a dime to any charity, take a few minutes to do a little research.
- There are sites specifically designed for this purpose, including [Charity Navigator](#), [Guidestar](#), and [Charity Watch](#).

Facebook Continued

- **Facebook quizzes and games**
- All those “getting to know you better” and “just for fun” quizzes you see on Facebook seem innocent enough.
- These 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 different damage](#) beyond simply taking over your Facebook account.

Facebook Continued

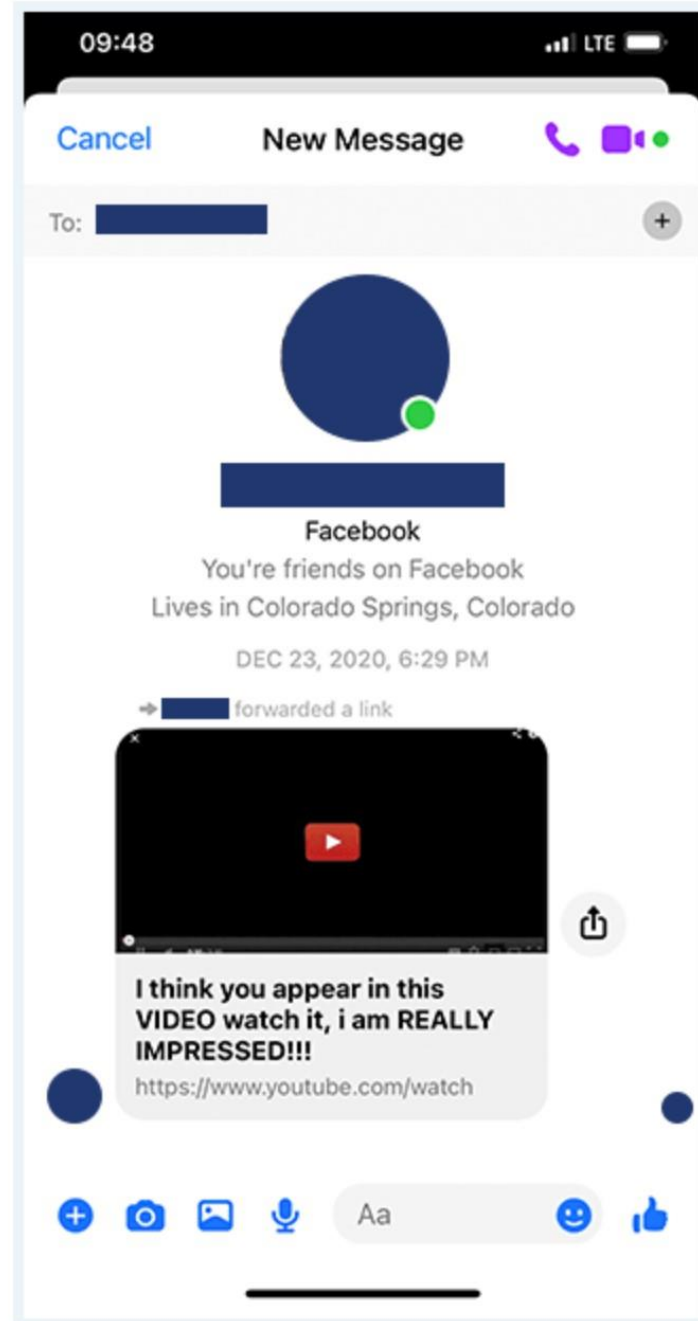
- **Fake friend requests**
- Anyone who's been on Facebook for a while has encountered this scam.
- You get a Facebook friend request from someone you swear you are already friends with.
- This is a favorite tactic by scammers, who **replicate entire Facebook accounts to mimic a legitimate person.**
- When you accept a fake request, you give the scammer insider access to you, even if you have your Facebook account locked down.
- They 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.

Facebook Continued

- **Suspicious links about you**
- 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) to **send malware links.**

The purpose? 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.**



Facebook Continued

- **Nonexistent coupons and discounts**
- Another tried-and-true tactic 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](#). 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 in order 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.
- The one thing these malicious apps don't do? Give you any discounts or coupons.

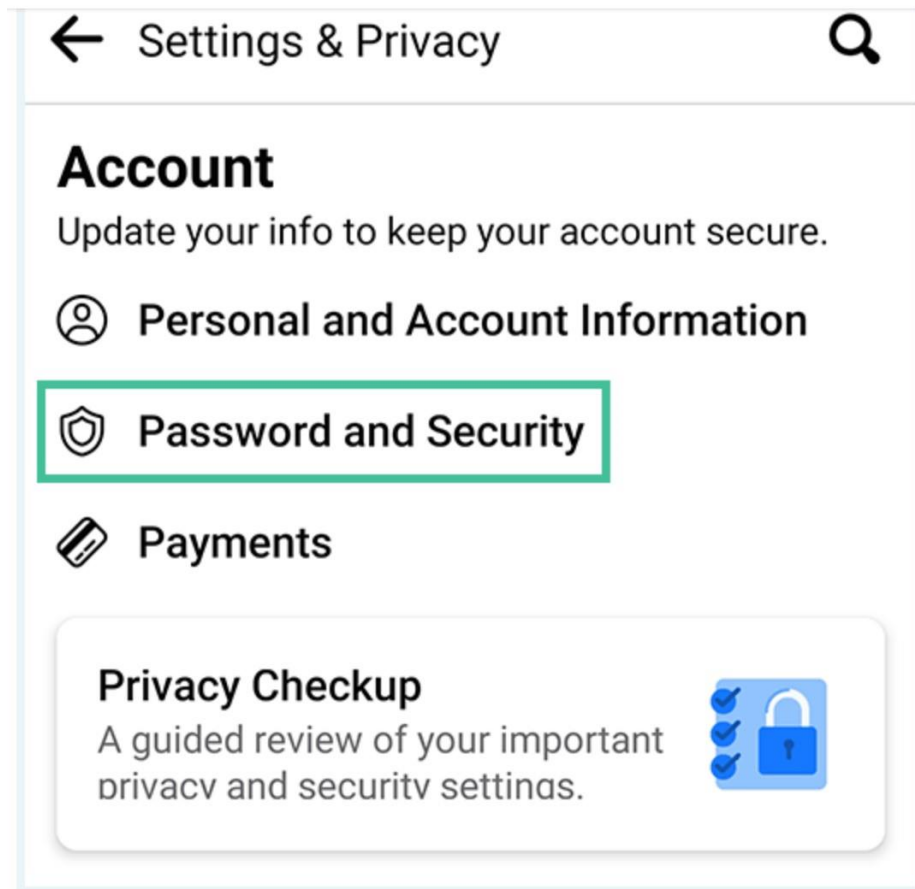
How to Avoid Scams on Facebook

- There are many things you can do to maintain your safety and avoid becoming a victim.
- **Things you can do within Facebook**
- From within Facebook, follow these best practices to avoid fraudsters.
- **1. Lock down your Facebook privacy settings**
- 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 friends list.

How to Avoid Scams on Facebook

- You can also tweak your privacy settings in other ways to keep your account safe. Here is how to do so from your computer:
 1. Open the Facebook app.
 2. Click on the down arrow (on iPhone) or hamburger menu (on Android) in the upper right corner of the screen.
 3. Choose **Settings & Privacy** from the menu.
 4. 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.

How to Avoid Scams on Facebook

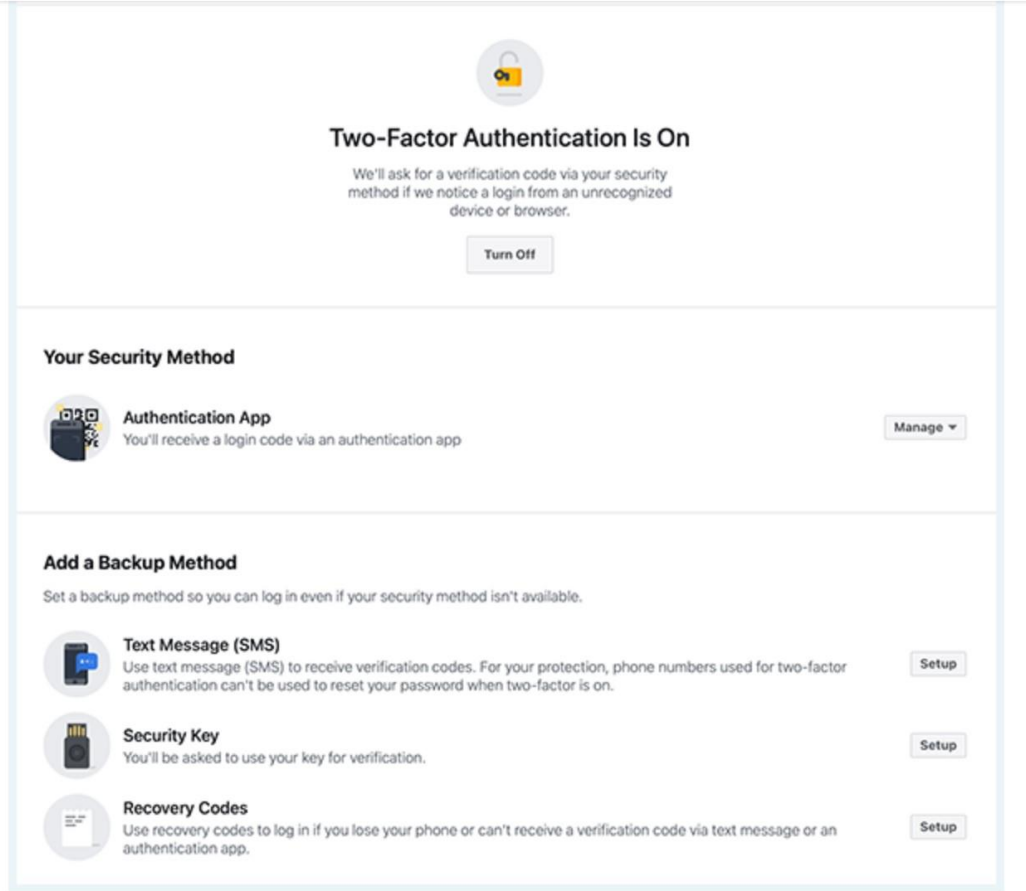


How to Avoid Scams on Facebook

- **2. Enable two-factor authentication**

- 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 your username and password**.
- This code is sent to your phone via text message or through an authenticator app.
- To **set up two-factor authentication on Facebook**, do the following:
 1. Open the Facebook app on your computer.
 2. Click on the down arrow in the upper right corner of the screen.
 3. Choose **Settings & Privacy > Settings > Security & Login**.
 4. 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.

How to Avoid Scams on Facebook




The screenshot shows the Facebook Two-Factor Authentication settings page. At the top, there is a lock icon and the heading "Two-Factor Authentication Is On". Below this, a paragraph explains that a verification code will be requested from unrecognized devices or browsers. A "Turn Off" button is provided. The page is divided into sections: "Your Security Method" and "Add a Backup Method". Under "Your Security Method", the "Authentication App" is listed as the active method, with a "Manage" dropdown. The "Add a Backup Method" section includes three options: "Text Message (SMS)", "Security Key", and "Recovery Codes", each with a "Setup" button.

Two-Factor Authentication Is On

We'll ask for a verification code via your security method if we notice a login from an unrecognized device or browser.


[Turn Off](#)


Your Security Method


 **Authentication App**
You'll receive a login code via an authentication app [Manage](#)

Add a Backup Method

Set a backup method so you can log in even if your security method isn't available.

 **Text Message (SMS)**
Use text message (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor is on. [Setup](#)

 **Security Key**
You'll be asked to use your key for verification. [Setup](#)

 **Recovery Codes**
Use recovery codes to log in if you lose your phone or can't receive a verification code via text message or an authentication app. [Setup](#)

How to Avoid Scams on Facebook

- **3. Decline a friend request from anyone you don't know**
- 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.

How to Avoid Scams on Facebook

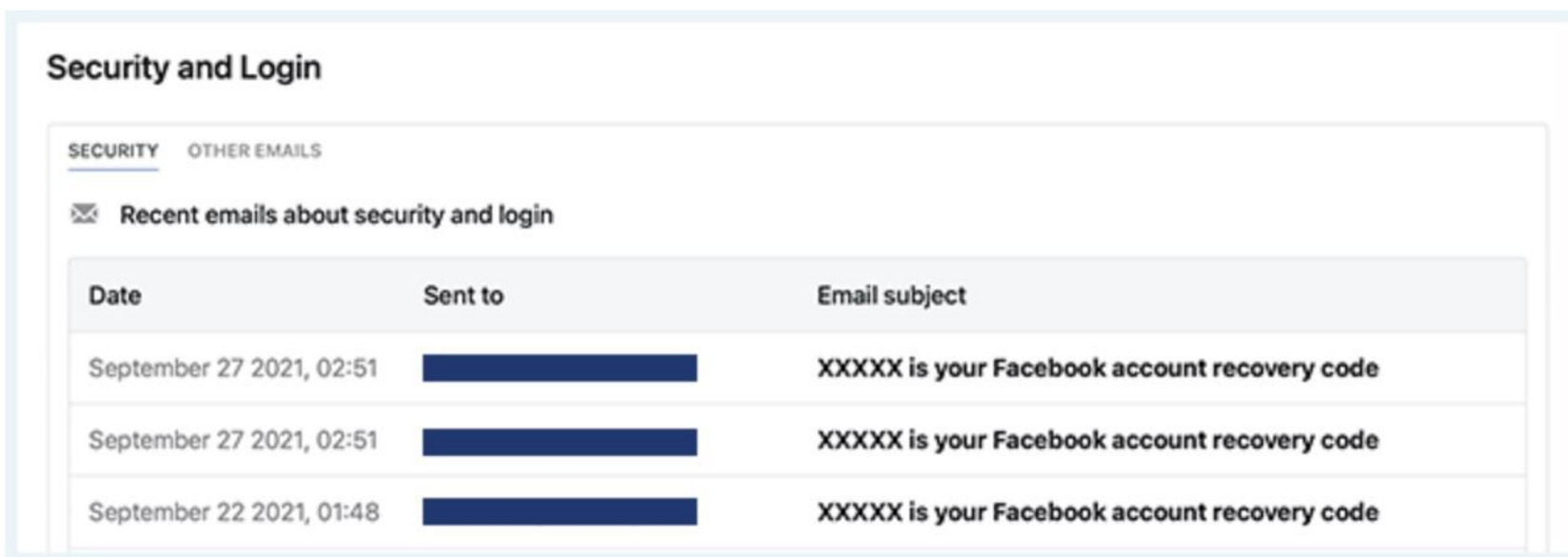
- **4. Ignore messages asking for personal information or money**
- If you receive a private message from someone you know and they're pleading for help (usually in the form of money), **double-check with this friend off Facebook to verify the legitimacy of their request.**
- Logically, if a real friend 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.

How to Avoid Scams on Facebook

- **5. Don't click on suspicious links sent to 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.
- Think about it. 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 here:

How to Avoid Scams on Facebook

1. Open the Facebook app on your computer.
2. Click on the down arrow in the upper right corner of the screen.
3. Choose **Settings & Privacy > Settings > Security & Login**.
4. Scroll down to **Advanced** and click **Recent Emails from Facebook**.



The screenshot shows the 'Security and Login' settings page on Facebook. It features two tabs: 'SECURITY' (selected) and 'OTHER EMAILS'. Below the tabs is a section titled 'Recent emails about security and login' with an envelope icon. A table lists three recent emails, all with the subject 'XXXXX is your Facebook account recovery code'.

Date	Sent to	Email subject
September 27 2021, 02:51	[REDACTED]	XXXXX is your Facebook account recovery code
September 27 2021, 02:51	[REDACTED]	XXXXX is your Facebook account recovery code
September 22 2021, 01:48	[REDACTED]	XXXXX is your Facebook account recovery code

How to Avoid Scams on Facebook

- **6. Check your login history regularly**
- Be sure to keep an eye on **all the places and devices that are logged in to your Facebook account**. This helps you get rid of unwanted access quickly.
- Here's how to **check your log-in sessions**.
 1. Open the Facebook app on your computer.
 2. Click on the down arrow in the upper right corner of the screen.
 3. Choose **Settings & Privacy > Settings > Security & Login**.
 4. Scroll down to **Where You're Logged In** and review for accuracy. Delete any suspicious logins.

How to Avoid Scams on Facebook

Where You're Logged In

-  **Mac - Unknown location**
Safari - **Active now**
-  **iPhone 11 Pro Max - Unknown location** 
Messenger for iOS - 3 minutes ago
-  **iPhone 11 Pro Max - [Redacted]** 
Facebook app - 2 hours ago

 [See Less](#) [Log Out Of All Sessions](#)

How to Avoid Scams on Facebook

- **7. Use a strong password**
- 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.

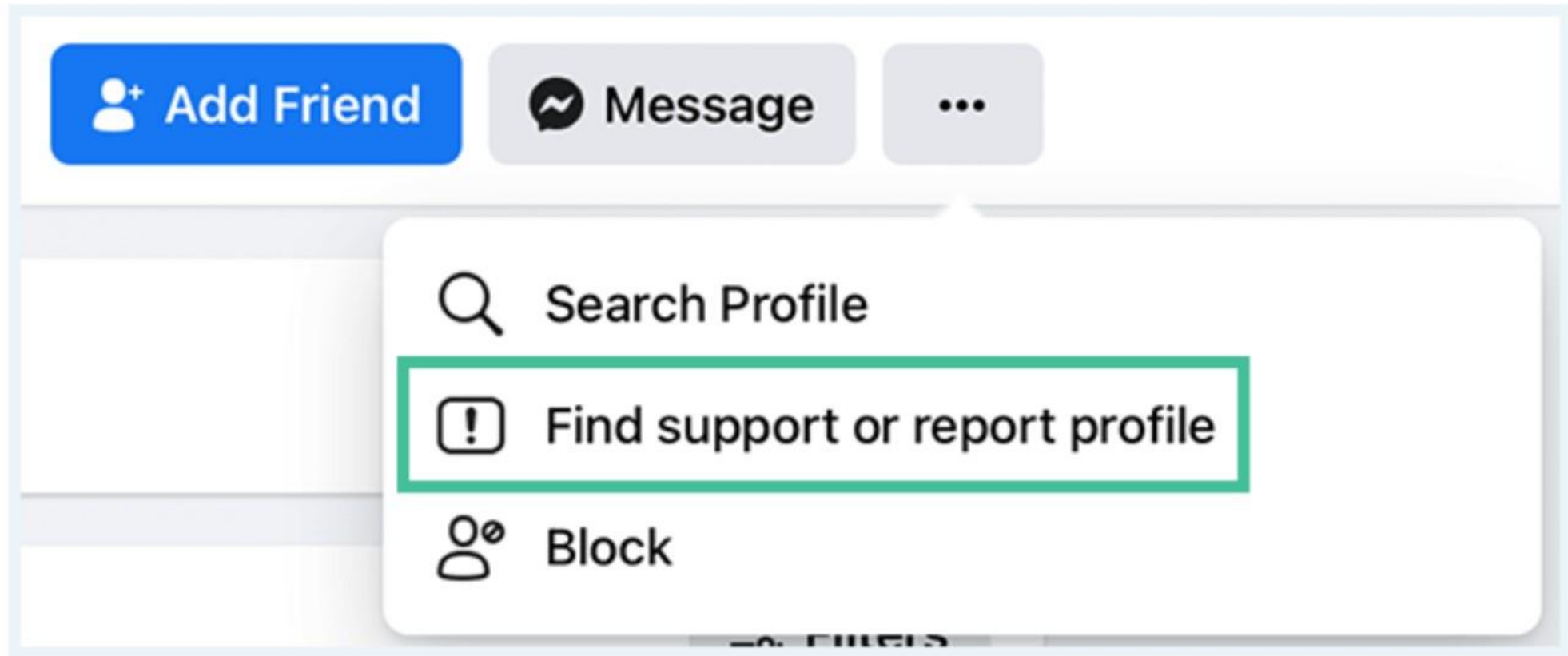
How to Avoid Scams on Facebook

- **8. Only shop from verified brand accounts**
- 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.

How to Avoid Scams on Facebook

- **9. Search regularly for accounts in your name**
- 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.**

How to Avoid Scams on Facebook



NOW you know how to protect yourself
online

Its your turn with your 10,000
Questions!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!