Is a stranger contacting you out of the blue?

You might be the target of a catfish or romance scammer. Here are some easy ways to determine if your new "friend" is really just someone trying to steal your identity or money:

1 Be wary of unexpected invitations to connect from total strangers, especially if the profile picture is very attractive, the person lives a long distance from you or is not within your age group.

2 If your new acquaintance seems to have a lot in common with you, think twice. This is how catfishers build an emotional relationship with you.

3 If the new friend can never meet, talk live on the phone or have a video conference with you, that's a red flag.

Want more information?

Check out this YouTube video at **oasisnet.org/safety**.

Notes

Thinking about paying with a gift card?

Think again. Gift cards are convenient, but it's important to remember that the gift cards are meant for gifts, not payments, fines or any other financial transactions with someone who contacts you online. Here's why:

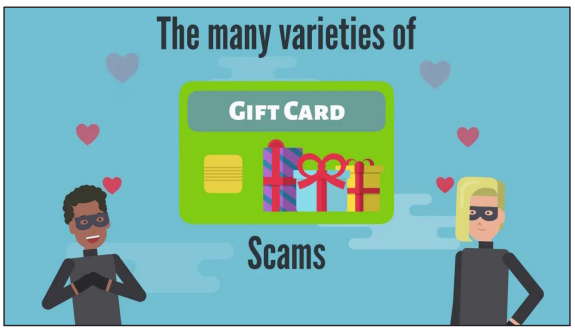
1 Gift cards are the number one form of payment demanded by scammers. This is because gift cards can be redeemed for cash from anywhere in the world.

2 Gift card scammers can remain anonymous while pocketing your money. Gift cards are almost like cash. Once you buy a gift card and share the serial number with a scammer, your money is gone forever.

3 There are hundreds of gift card scams, but some of the most popular ones are scammers posing as computer tech support, the IRS, the police or a utility company.

Want more information?

Check out this YouTube video at **oasisnet.org/safety**.



Notes

Ready to donate?

Do your homework first. When we hear about catastrophic events in the news, our first inclination is to open our hearts and wallets to help. Scammers pay attention to disastrous events, too. To avoid charity fraud, be sure to check out the organization online for clues that you are giving to a legitimate cause.

1. Check out the organization's website. Look for positive and negative feedback, and history of engagement.

2. Look for websites that publish charity ratings, which are based on an organization's financial transparency, compliance with nonprofit best practices and more. Look for Charity Navigator, GuideStar and the BBB Wise Giving Alliance.

3. Search social media accounts of the organization. Look for pictures, videos and stories and stakeholder and volunteer engagement.

Want more information?

Check out this YouTube video at **oasisnet.org/safety**.

Notes

Lost your phone?

You're not alone. Over 5 million smart phones are lost or stolen every year. To protect the data and personal information on your phone or tablet, follow these easy steps:

1 Set a passcode or PIN to prevent a criminal from getting access to private information stored on your device. Some smartphones offer fingerprint or facial recognition, but it all starts with a passcode.

2 Create a lockscreen message asking the finder to call or email you if the phone is found.

3 Set up your device to use the finder apps to locate your lost device. On an iPhone, go to Settings and turn on Find my iPhone. On an Android, go to Settings and turn on Find my Device. Both Apple and Android have apps to help you locate and secure or erase your device remotely.

Want more information?

Check out this YouTube video at **oasisnet.org/safety**.

Notes

Wondering if social media is safe?

Social media is a great way to stay in touch with friends and family and to follow your favorite organizations, interests and causes. But there are some risks. Here are just a few things to keep in mind to make sure you are using your favorite social media channels safely:

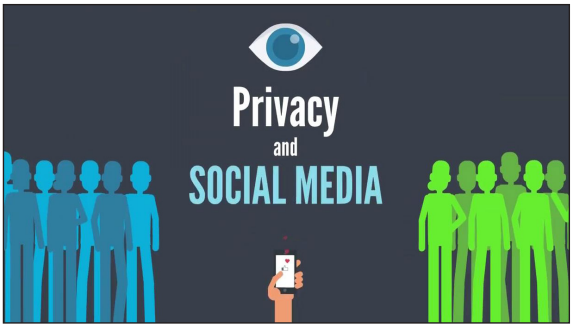
1. Social media is not necessarily private. Even if you share a message or photo with someone privately, you lose control as soon as it's in someone else's hands. Assume that everything you share on social media has the potential to be public. This includes sharing your whereabouts and when you are out of town.

2. Not all social media contacts are genuine. Anyone can create a social media account and call themselves by any name. Scammers often clone existing real accounts in order to get personal information.

3. Think twice before you participate in social media surveys. They can seem harmless, but they can be a way for scammers to initiate a conversation with you. Make sure you are confident of the source of the survey before you fill it out.

Want more information?

Check out this YouTube video at **oasisnet.org/safety**.



Notes