Safety Tips

In order to stay safe in the crypto space we first need to understand where and how we can get attacked. So we will talk about some of the most common attacks you can prevent or protect yourself as well as discussing some tips to protect yourself from each attack.
Seed phrase compromise

Smart contract risk

Smart contracts can have security breaches that can drain your account. Usually wallets warn you of some of these breaches, but you should always check yourself every smart contract you interact with on a site like de.fi or one with a similar service that scans the smart contract for you and shows you everything that could be a potential liability

Rug pulls

A rug pull is essentially when a team dumps everything on the holders and disappears making profit on all the money invested by the people that trusted the project. You should always do your own research on the project and the team behind it before investing on it, if the team is shady or the tokenomics don't make sense then it is not recommendable to invest on it because the chances of a rug pool are high.

Honeypots

Honeypots are scams that involve a situation where you can get a lot of money if you invest a small amount first to be able to win that money, but in reality you end up losing your money invested and you win nothing in return. These scams take the form of someone pretending to be a crypto novice asking for a favor and then exposing their seed phrase for an wallet with tons of money but no tokens for gas fees or a smart contract with an obvious exploit that needs you to put a bit of money in the contract to access the exploit. In both situations the moment you put the money the scammer transfers it to a safe wallet. The best way to avoid these types of scams is to be ethical and not try to win some easy cash when it looks too good to be true.

Phishing

This type of scam involves the scammer sending you a malicious link that sends you to a fake website where they will ask you for valuable information such as seed phrases. This link could even download a virus that could scan your computer for that information or read your keyboard inputs to get the information once you type it in. To avoid this type of scams you should always double check before clicking on a link and if it seems suspicious in any way you shouldn't click it.

Social Media giveaway scams

Scammers usually post fake giveaways on social media in order to lure greedy people, however when clicking on the link of the giveaway the site asks you to prove that your account is legitimate (usually making you sing a smart contract). This scam is a form of phishing and usually involves smart contract risk, but it is so common I decided to mention it as its own category. To avoid it check the account doing the giveaway, if it is not an official account or it looks like a shady team avoid it as it’s probably a scam.

Ponzi schemes

Ponzi schemes pay older investors with the proceeds from new ones. To get fresh investors, cryptocurrency scammers will lure new investors with bitcoin. It's a scheme that runs in circles, since there are no legitimate investments; it is all about targeting new investors for money. The main lure of a Ponzi scheme is the promise of huge profits with little risk. If a deal looks too good to be true it probably is too good to be true, the best way to avoid these types of scams is to do proper research before investing and understanding that easy and quick money is **always** a lie.

Fake exchanges

Some scammers build similar looking pages for well known exchanges or lure novice crypto users to fake exchanges with the promise of great rewards. To avoid falling for this trap stick to the well known and established exchanges and use apps like defillama or twitter to find and access the real exchange.

Employment offers and fraudulent employees

Scammers will also impersonate recruiters or job seekers to get access to cryptocurrency accounts. With this ploy, they offer an interesting job but require cryptocurrency as payment for job training. Again the best way to avoid this trap is to do proper research on the company or the person contacting you, usually real companies do not require payments to train you.

Conclusion

Most of these attacks can be prevented if we use common sense and don’t get greedy, the rest can be prevented by being diligent and doing proper research before taking action. So in order to stay safe on the crypto market one has to be disciplined enough to make the research needed and not get greedy when encountering an offer that seems to be too good to be true (because most probably it is a scam)