Top 50 Ways To Avoid Getting Scammed

Updated for 2019

1. When making a purchase or investment, always use a credit card. This gives you protection provided by the card companies who have built in fraud protection.
   Source: Visa

2. On the same token, never make a payment via wire transfer. It is almost impossible to get back in a case that fraud is discovered.
   Source:FTC

3. Never make a payment using cryptocurrency. This has even less protection than a wire transfer.
   Source: Finder.com

4. Use Paypal. Paypal offers even greater protection to their users than Visa & Mastercard.
   Source: PayPal Protection

5. Do not make payments via Western Union or Money Gram. This is the same as cash and cannot be recovered in case of a scam.
   Source: FTC

6. Do not give control of your computer via a screen sharing service like Teamviewer unless you trust the other party intimately. Doing this can give an opportunity for a scammer to install malware on your machine:
   Source: Scam Watch

7. Stay alert. Internet scams are on the rise and account for billions of dollars in losses every year. By paying attention whenever engaging in a transaction, you can reduce the risk of becoming a victim.
   Source: Norton

8. Never give out personal information like card details, bank accounts, id card numbers, etc to someone who calls you unless the phone number is recognized. Otherwise, politely hang up. Then, look up the company online and locate their phone. Call back and only then, provide your info.
   Source: Money Advice Service

9. Do not confirm or deny information over the phone. Scammers frequently call and say that they just want to confirm your details. This can be a trick. Be aware.
   Source: ScamWatch

10. The one ring scam: If you receive a missed call from an out of area code number, don't call it back. A common scam is that the phone number appears to be from the US, but is actually international "900". When you call back, your phone bill is charged with exorbitant fees.
    Source: FCC

11. Try to avoid using non bank ATM's. They are more likely to be rigged by criminals to steal your card info. Instead use the banks.
    Source: PC Mag

12. In any case, when withdrawing money from an ATM, move your body close to the machine, then use your hands to shield the keypad when entering the pin code to avoid prying eyes:
    Source: UK Police

13. Do not leave your credit cards laying around. Don't be easy prey for credit card thieves who can easily take a photo of your card and use it later.
    Source: Credit Card Insider

14. When using your credit card to pay for something in person, don't leave it out for longer than necessary. This reduces the chances of it being photographed by a thief, or picked up on a camera.
    Source: Credit Card Insider

15. If you lose your credit card, call your bank and cancel it. If you aren't sure if it is lost, call your bank and ask them to put a pause on the card until you call them back when you locate it.
    Source: Money Crashers

16. Keep a copy of all your credit and debit cards (front and back) in a secure place just in case they are lost or stolen. This way, you can easily locate the phone number on the back of the card so you can all the bank to pause or cancel it.

Source: Lifelock

17. Before making a payment on the web, always check the browser. The last word before the extension is the actual site you are on. For example, if you are on google.fraud.com, then you are not actually on Google.com. Instead, you are on fraud.com. Make sure you are where you expect to be.
    Source: ScamWatch

18. Before entering in personal or payment details on a site, always check to see the green lock button on the top left of the browser (to the left of the website url). If it is green, this means that information entered is encrypted and secure. If not, do not enter your info.
    Source: Google

19. Buying from a new website? Always search the company name with the word “reviews” next to the company name. There are plenty of lies on the web but if people are complaining, be aware.
    Source: pewinternet

20. Also search the company name with the word “scam” next to the company name.
    Source: pewinternet

21. If an email or text looks suspicious, do not open it. Sometimes, just opening it can give a thief access to your personal information. Instead, delete it.
    Source: ASIC

22. Password protect your devices. This can make it more difficult for scammers to gain access.
    Source: FTC

23. Speaking of passwords. Use secure passwords! Using things like your birthday, the name of a loved one or the street you grew up on is not secure and can easily be figured out by a thief. If you aren’t sure how to create a secure password, let Google Chrome do it for you. When making a new password, right click in the password box and choose “suggest password” from the menu.
    Source: Google

24. Alternately, a secure password creation method I like to use is the following: Think of a sentence that is deeply personal and reflects something known only to you. For example: “I have a secret crush on that cute guy who works down the hall.”. Next, take the first letter of each word in the sentence so you have this: ihascotcgwwdth. Then, capitalize one or two important words so maybe “crush” and “guy” so your password looks like this: ihasCotcGwwdth. And finally, add in a number and a symbol like this: ihasCotcGwwdth2&. So now you have a secure password you can easily remember

because it is a meaningful sentence.
Source: Article author. Pierce Wilson.

25. Dating scams are very common as well. Let's say you meet someone on the internet and they start flirting with you. Then, later, or the next day, or even weeks or months later, they ask you for money. Be aware.
    Source: FTC

26. The IRS will never call you and ask for personal information. If someone calls you from the IRS and warns you about a tax debt. It is a scam.
    Source: IRS

27. Interested in investing? Make sure your broker is licensed. Find their license number, and look them up on relevant government body like Cysec or Finra.
    Source: Investopedia

28. Trading online? There are hundreds, maybe even thousands of fraudulent brokers on the web. Make sure to look up a broker before using them by typing in the name of the brokerage with the word "scam" next to the company name. Where there is smoke, there is fire.
    Source: SEC

29. What about regulated brokers? They can scam people too. Did the brokerage give you a test to make sure you are qualified to trade? This is an absolute requirement. Is your broker giving you investment advice? This is illegal. In many cases, legally registered brokerages win when their clients lose and will deliberately provide bad advice to help their clients lose!
    Source: https://www.forexpeacearmy.com

30. Have you looked at your social media privacy settings lately? Many people are unaware how public their info they post is. Carefully review your privacy setting to ensure that you aren't sharing private information with the public that can later be used to cyber criminals to target you.
    Source: Norton

31. Don't trust your caller ID. Scammers use technology to fake the numbers they are calling from leading to believe they are calling from a known business or organization. If they are asking for personal or payment info, politely tell them you will call becak when it is more convenient, then call back the correct number just to be sure.
    Source: FTC

32. If you receive a call that you won a prize. Be alert. If you never signed up, it is probably a scam. Sometimes, they will use this opportunity to ask for card details so you can "pay

for shipping". Then they will use your card fraudulently.
Source: Walmart

33. Stay in the loop. Sign for free scammer alerts provided by the ftc. You can do so here: http://www.ftc.gov/scams
Source: FTC

34. Someone asking you to deposit a check and wire money back? It is a scam. Don't do it. Even if the funds clear from the check into your account, they will disappear when the bank discovers the fraud and you will be out the check and the wire transfer.
Source: FTC

35. Got an email about an inheritance you may be entitled to from a lawyer? It is a common scam. Do not respond to any further emails and do not give over any personal information or send any money.
Source: AARP

36. Scammers are often much more devious than you can imagine. They will take the time to get to know you, become a friend, and gain your trust before tricking you into parting with your money. Don't ignore the red flags. If something seems off, it probably is. Seek the advice of family and friends if you aren't sure.
Source: Times of Israel

37. If it sounds too good to be true, it is. No, you cannot make $20,000/week with only 3 hours of work from your bed. No, you will not get rich trying to sell your friends soap in a pyramid scheme. If these things worked and were easy, EVERYONE would be doing them. The reason they aren't is because they are simply not true.
Source: FTC

38. Not a pyramid scheme? Sure. Since "Pyramid Scheme" has gotten such a bad reputation, as well as MLM or multi-level marketing, they have switched the name again. Now, it is called Network Marketing, Direct Selling, and even Referral Marketing. Only very, very successful members at the top of the scheme make any real money. You might be able to make a few bucks hustling your friends and family but don't expect to get rich in just a few hours a week.
Source: ArtofManliness

For Businesses

39. Always ship to the billing address of the cardholder. This prevents the common claim of thieving customers that they never got the package.

Source: Authorize.net

40. Make sure there is an AVS match to the address when you ran the credit card. This ensures that the credit card matches the provided address so you know you are shipping to the card holder.
    Source: Authorize.net

41. If shipping to an address other than the billing address, use a service like eye4fraud to insure you against fraud. This way, if it turns out that the card was fraudulent, you are fully insured.
    Source: Eye4Fraud

42. Always use tracking with delivery confirmation. This way, if a dishonest customer opens a chargeback, you have proof that the product was delivered.
    Source: Chargebacks911

43. When paying vendors via wire transfer, always confirm the details verbally with the financial controller. Scammers will hack into the CEO or FCO's email and then request a wire transfer that looks legitimate but is actually fraudulent.
    Source: SBCP Bank

44. Just because you are a business, doesn't mean you can't fall victim to fraud. Always check new vendors out. Read reviews. Do your due diligence.
    Source: Incorp

45. An SEO company promise you guaranteed 1st page results on Google for a flat fee? This is a scam. Google does not sell this spot to anyone. It simply is not for sale so anyone promising you this is not being honest.
    Source: SEO Expert Brad

46. A client overpay via check and asking you to wire the difference to them? This is a scam. Do not wire the money. The check is most likely stolen and the funds will be withdrawn from your account. Wiring the difference to the client will only make matters worse.
    Source: ScamWatch

47. Check every invoice before you pay it. Some thieves simply send fake invoices to many companies in the hope that it will slip through the cracks. Check every invoice before paying it.
    Source: Fraud Financial Action

48. Use restricted access for employees. Do not give an employee more access than they need to your accounts, or to customer information. This can reduce your risk in case the employee is dishonest.

Source: DarkReading.com

49. Letting an employee go? Make sure to change any passwords they have access to. This can help ensure they don't harm you, defraud you, or your customers.
    Source: Druva

50. Under the gun? Bills due? Feeling the pressure? Don't make any quick financial decisions. Scammers are trained to take advantage of people in vulnerable situations so be doubly careful. Take more time to think things through. Speak to family, friends or mentors before making any consequential moves.
    Source: FTC