Personal Safety

The overwhelming majority of FAVORZ users are trustworthy and well-meaning.

Millions of violent crimes occur in the U.S. each year: 10,000+ homicides, 600,000+ robberies, 5 million assaults.

Please take the same common sense precautions online as you would offline.

When meeting someone for the first time, please remember to:

- Insist on a public meeting place like a cafe, bank, or shopping center.
- Do not meet in a secluded place, or invite strangers into your home without caution.
- Tell a friend or family member where you're going.
- Take your cell phone along if you have one.
- Consider having a friend accompany you.
- Trust your instincts.

Taking these simple precautions helps make FAVORZ safer to use for everyone.

For more information about personal safety online, check out these resources:

- http://www.staysafeonline.org/
- http://www.onguardonline.gov/
- http://getsafeonline.org
- http://wiredsafety.org

Prohibited

Users must comply with all applicable laws, the FAVORZ terms of use, and all posted site rules.

Here is a partial list of goods, services, and content prohibited on FAVORZ:

- weapons; firearms/guns and components; BB/pellet, stun, and spear guns; etc
- ammunition, clips, cartridges, reloading materials, gunpowder, fireworks, explosives
- offers, solicitation, or facilitation of illegal prostitution and/or sex trafficking

- exploitation or endangerment of minors; child pornography
- recalled items; hazardous materials; body parts/fluids; unsanitized bedding/clothing
- prescription drugs, medical devices; controlled substances and related items
- alcohol or tobacco; unpackaged or adulterated food or cosmetics
- pet sales (re-homing with small adoption fee ok), animal parts, stud service
- endangered, imperiled and/or protected species and any parts thereof, e.g. ivory
- false, misleading, deceptive, or fraudulent content; bait and switch; keyword spam
- offensive, obscene, defamatory, threatening, or malicious postings or email
- anyone's personal, identifying, confidential or proprietary information
- food stamps, WIC vouchers, SNAP or WIC goods, governmental assistance
- stolen property, property with serial number removed/altered, burglary tools, etc
- ID cards, licenses, police insignia, government documents, birth certificates, etc
- US military items not demilitarized in accord with Defense Department policy
- counterfeit, replica, or pirated items; tickets or gift cards that restrict transfer
- lottery or raffle tickets, sweepstakes entries, slot machines, gambling items
- spam; miscategorized, overposted, cross-posted, or nonlocal content
- postings or email the primary purpose of which is to drive traffic to a website
- postings or email offering, promoting, or linking to unsolicited products or services
- affiliate marketing; network, or multi-level marketing; pyramid schemes
- any good, service, or content that violates the law or legal rights of others

Please don't use FAVORZ for these purposes, and report anyone else you see doing so.

Thanks for helping keep FAVORZ safe and useful for everyone.

Avoiding Scams

Deal locally, face-to-face —follow this one rule and avoid 99% of scam attempts.

- Do not provide payment to anyone you have not met in person.
- Beware offers involving shipping - deal with locals you can meet in person.
- Never wire funds (e.g. Western Union) - anyone who asks you to is a scammer.
- Don't accept cashier/certified checks or money orders - banks cash fakes, then hold you responsible.
- Transactions are between users only, no third party provides a "guarantee".
- Never give out financial info (bank account, social security, paypal account, etc).
- Do not rent or purchase sight-unseen—that amazing "deal" may not exist.
- Refuse background/credit checks until you have met landlord/employer in person.
- "FAVORZ voicemails" - Any message asking you to access or check "FAVORZ voicemails" or "FAVORZ voice messages" is fraudulent - no such service exists.

Who should I notify about fraud or scam attempts?

United States

- Internet Fraud Complaint Center
- FTC complaint form and hotline: 877-FTC-HELP (877-382-4357)
- Consumer Sentinel/Military (for armed service members and families)
- SIIA Software and Content Piracy reporting
- Ohio Attorney General Consumer Complaints
- New York Attorney General, Avoid Online Investment Fraud

Canada

- Canadian Anti-Fraud Centre or 888-495-8501 (toll-free)

If you are defrauded by someone you met in person, contact your local police department.

If you suspect that a FAVORZ post may be connected to a scam, please send us the details.

Recognizing scams

Most scams attempts involve one or more of the following:

- Email or text from someone that is not local to your area.
- Vague initial inquiry, e.g. asking about "the item." Poor grammar/spelling.
- Western Union, Money Gram, cashier check, money order, Paypal, Zelle, shipping, escrow service, or a "guarantee."
- Inability or refusal to meet face-to-face to complete the transaction.

Examples of Scams

1. Someone claims your transaction is guaranteed, that a buyer/seller is officially certified, OR that a third party of any kind will handle or provide protection for a payment:

- These claims are fraudulent, as transactions are between users only.

- The scammer will often send an official looking (but fake) email that appears to come from FAVORZ or another third party, offering a guarantee, certifying a seller, or pretending to handle payments.

2. Distant person offers a genuine-looking (but fake) cashier's check:

- You receive an email or text (examples below) offering to buy your item, pay for your services in advance, or rent your apartment, sight unseen and without meeting you in person.
- A cashier's check is offered for your sale item as a deposit for an apartment or for your services.
- Value of cashier's check often far exceeds your item—scammer offers to "trust" you, and asks you to wire the balance via money transfer service.
- Banks will cash fake checks AND THEN HOLD YOU RESPONSIBLE WHEN THE CHECK FAILS TO CLEAR, sometimes including criminal prosecution.
- Scams often pretend to involve a 3rd party (shipping agent, business associate, etc.).

3. Someone requests wire service payment via Western Union or MoneyGram:

- Deal often seems too good to be true, price is too low, or rent is below market, etc.
- Scam "bait" items include apartments, laptops, TVs, cell phones, tickets, other high value items.
- Scammer may (falsely) claim a confirmation code from you is needed before he can withdraw your money.
- Common countries currently include: Nigeria, Romania, UK, Netherlands—but could be anywhere.
- Rental may be local, but owner is "travelling" or "relocating" and needs you to wire money abroad.
- Scammer may pretend to be unable to speak by phone (scammers prefer to operate by text/email).

4. Distant person offers to send you a cashier's check or money order and then have you wire money:

- This is ALWAYS a scam in our experience—the cashier's check is FAKE.
- Sometimes accompanies an offer of merchandise, sometimes not.
- Scammer often asks for your name, address, etc. for printing on the fake check.
- Deal often seems too good to be true.

5. Distant seller suggests use of an online escrow service:

- Most online escrow sites are FRAUDULENT and operated by scammers.
- For more info, do a google search on "fake escrow" or "escrow fraud."

6. Distant seller asks for a partial payment upfront, after which they will ship goods:

- He says he trusts you with the partial payment.
- He may say he has already shipped the goods.
- Deal often **sounds too good to be true**.

7. Foreign company offers you a job receiving payments from customers, then wiring funds:

- Foreign company may aim it is unable to receive payments from its customers directly.
- You are typically offered a percentage of payments received.
- This kind of "position" may be posted as a job, or offered to you via email.

Unlawful sales of recalled items are prohibited

Please be sure items are safe to use and legal to sell.

United States:

- Consumer Product Safety Commission (cpsc.gov)
- Reseller's Guide to Selling Safer Products
- SaferProducts.gov (saferproducts.gov)
- Recalls.gov (recalls.gov)
- Safercar.gov (safercar.gov)

CA: Health Canada Consumer Product Safety (hc-sc.gc.ca)

UK: Royal Society for the Prevention of Accidents (rospa.com)

EU: European Union Consumer Safety (ec.europa.eu)

AU: Product Safety Australia (productsafety.gov.au)

Phishing stealing accounts, passwords, or financial information by masquerading as a trusted party.

Phishers may email you an official looking email with a link to a real looking (but fake) FAVORZ site. If you type your login and password into the fake CL site, the phisher can then use your account to post scam ads on CL.

How phishing works:

1. You receive a supposedly official email from FAVORZ, asking you to confirm your password, username, phone number, or credit card information.

    - This email may threaten you with the removal of your posts or the closure of your account if you do not comply immediately.
    - If the sender is using email spoofing, the message may appear to come directly from FAVORZ.

2. You click the link in the email and are taken to a fraudulent third-party site that may resemble a legitimate FAVORZ page.

3. You may be asked to download an attachment, install specific software, or receive a message to your phone.

4. You enter your login information on the fraudulent page, inadvertently providing it to a third party.

5. The third party scammer can then use the information you provided to gain access to your actual FAVORZ account.

How to avoid phishing attempts and protect your account information

- Never click on email links that ask you for any personal or account information.
- Make sure to login to your account only by navigating manually to FAVORZ.com.
- If you are unsure about the status of your account or your posts, the safest way to check is to go directly to FAVORZ.com and login.
- If you do not see any problems within your account, you can safely ignore any messages to the contrary.
- Never provide a phone authentication code to anyone else.
    - FAVORZ will only ask for you to enter it on our site as part of the posting process.

- Use common sense. If an email seems suspicious, fishy, or too good to be true. . . it probably is!

Think you've been phished?

If you see strange activity or unfamiliar posts on your account page, please change your password immediately and manually delete any pending requests.

If you use the same password for your email account (or any other services), you may want to change those passwords as well.

Harassment, publication of personal information

If your personal information has been posted on FAVORZ, use our online form to report the issue.

Abusive email

If you receive an abusive email from an address that ends with reply.FAVORZ.com, for example:

rcc9la26d7534400a6a03514c34f9200@reply.FAVORZ.com

locate and use the last link that appears at the bottom part of that message:

"Please flag unwanted messages (spam, scam, other):"

If you are receiving email directly from another individual (i.e. you can see the sender's email address), it may be advisable to forward details of the messages, including the full email headers, to the sender's email account provider. If you feel the harassment is significant enough, it may make sense to report the issue to law enforcement as well. In addition, it may help to set up a block against the sender's email address in your email client.

Abusive postings

You can flag abusive postings using the flagging links provided.