PENNSYLVANIA STATE POLICE
COMMUNITY AWARENESS BULLETIN
CAB 001-26 May 8, 2026

SCAMS ASSOCIATED WITH MAJOR EVENTS

In 2026, Pennsylvania will be thrust in the spotlight for numerous high-profile events taking place across the state. The Pennsylvania State Police (PSP) is reminding residents and visitors to be aware that criminals will use major events to take advantage of unsuspecting victims. Criminals capitalize on high-profile occasions by utilizing various techniques to steal cash, personal information, and belongings. They may use stolen personal information to create fraudulent accounts to conduct further illegal activity. Listed below are potential scams and crimes likely to be committed by criminals throughout the duration of the upcoming events.

Counterfeit Merchandise: Be wary of websites or vendors located outside of event locations selling apparel and merchandise at prices below suggested retail value. Authentic merchandise is offered on official websites or within the event location and can be purchased using secure payment methods.

Ticket Scams: Criminals are likely to sell counterfeit tickets or fake digital tickets using social media or unofficial platforms. Only purchase tickets from verified platforms.

Accommodations Fraud: Be cautious of rentals, hotels, or travel packages offered at "too good to be true" prices. These may be scams that result in stolen deposits and compromised personal information.

Cell Phone Thefts: Criminals have been known to target unsuspecting victims for cell phone thefts during large-scale events. The phones may be stolen from pants pockets or even from small, zippered waist bags. The stolen phones are then wiped and shipped in bulk overseas.

Malware/Phishing: Social media may be used to send links to photos and videos of important event moments. The links may appear valid, but when clicked, malware is downloaded. There are legitimate websites and applications specifically designed for the events that can be utilized to obtain the most up-to-date and accurate information.

QR Codes: Fraudulent QR codes may be placed in areas surrounding event venues to mislead unsuspecting attendees into believing the link is for legitimate sites to purchase merchandise, tickets, parking, meet and greet opportunities, or other goods.

ATM Cash Traps/Skimming Devices: Attendees should use caution when using ATMs and points-of-sale terminals to withdraw funds or pay for goods.[1] These methods are easy ways for criminals to steal credit and debit card data, as well as cash.

Tips To Avoid Becoming a Victim While Attending Events:

- Stay vigilant in densely packed crowds.
- Use zippered pockets, front pockets, or specialized gear like a running belt.
- Ensure "Find My" is active on your phone.
- Never store phones in back pockets.
- Never click on a link or download an attachment unless you are positive it is legitimate. Even if the address of the sender appears correct, the address may have been “spoofed” to appear genuine.

- Only download apps from authorized stores.
- Become familiar with your peer-to-peer payment application policies related to fraud protection.
- When using an ATM, if the cash does not dispense immediately, report it.
- Avoid using standalone ATMs.
- Do not use an ATM if it shows signs of tampering.
- Check to determine whether the QR codes are stickers before you scan. This is a red flag the code may be fraudulent.
- Always check the URL of the website after scanning a QR code, and verify the website looks official.
- Make sure the website is secure. Look for the lock symbol and an "s" at the end of the "http" portion of the site's URL.
- Do not trust sites that ask for personal or payment information before allowing you to proceed.
- Pay with a credit card, not a debit card. You may have more leverage when disputing fraudulent charges.[2]
- Be cautious if the site does not have contact information for customer support issues.
- Do not make any purchases from scalpers.
- When searching for tickets online, confirm you know which company you are buying from and do not assume it is one of the more well-known options. Do not simply choose the first response at the top of your search results.
- Do not click on links or attachments in social media posts, emails, or texts.

If You Have Been the Victim of a Scam or other Crime:

- Contact your local law enforcement agency.
- File a complaint with the Internet Crime Complaint Center at http://www.ic3.gov.
- File a complaint with the Federal Trade Commission at https://reportfraud.ftc.gov/assistant or 1-877-FTC-HELP. If possible, be prepared to provide:
  - Your contact information: name, address, phone number, and email address.
  - The type of product or service involved.
  - Information about the crime: business name, address, phone number, website, email address, and representative's name.
  - Details about the transaction: amount paid, how you paid, and the date of the transaction.
- Report tips and suspicious activity to tips@pa.gov.

[1] Huffman, M. (2026, April 2). Beware the new ATM 'trap door' scam. *ConsumerAffairs*. Retrieved 04/21/2026 from https://www.consumeraffairs.com/news/beware-the-new-atm-trap-door-scam-040226.html.

[2] Oregon FBI tech Tuesday: Building a digital defense against fake ticket scams. *FBI*. Retrieved 04/21/2026 from https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-fake-ticket-scams.