NAVIGATING GAMING FRAUD

SAFEGUARDING YOUR EXPERIENCE

Online gaming has grown significantly in recent years, which has led to an increase in scams across various gaming platforms. While these platforms are a space for Veterans and the general population to build community, they are targets for fraudulent activity as well. In many cases, gaming companies provide minimal support when users experience financial harm or risks.

Common gaming fraud schemes include:

- Credit card fraud
- Account hacking attempts
- Account theft and takeovers
- Affiliate fraud paying out rewards to non-existent players
- Loss of gaming access from fraudulent activities
- Phishing attempts for personal identifiable information

DO'S

There are many ways to ensure gaming environments are kept safe and secure. When gaming or making purchases on gaming assets, consider the following to protect yourself:

- **Purchase products through verified companies.** This includes hardware, software, and digital assets. Refunds and support regarding gaming assets are more likely through verified venders than through non-verified.
- **Sign up for Multifactor Authentication (MFA).** This method of signing into your accounts uses additional measures to verify your identity which can protect you and your assets.
- **If possible, pay with credit cards instead of debit cards.** Credit cards can offer stronger fraud protections, such as reporting fraudulent activities and offering a refund from a scam.
- **Use a Virtual Private Network (VPN).** VPNs can ensure extra safety against cyber-attacks while protecting your IP address. They also perform system scans regularly to help block infected files and detect malware.
- **Avoid clicking suspicious links.** This includes links sent to you in a private message or in chat room environments. Remember, these can be phishing attempts, which aim to steal your personal information by posing as trusted sources.

DON'TS

Scammers and fraudsters will take any opportunity to make a profit in gaming environments. Consider the following items to protect you from losing gaming related assets:

- **Do not buy the lowest priced items or used items on all game-related purchases.** Unless through a verified vendor, fraudsters will utilize low prices as a gateway to make quick money on low quality products.
- **Do not share your password for any gaming accounts or social gaming tools.** This may include but not be limited to applications such as Steam, EA App, Battle.net, Epic Games, Discord, Twitch, etc.
- **Do not share personal information about yourself in voice chat and gaming chat rooms.** You should avoid using any personal identifying information including your name, location, date of birth, or any additional items about yourself.
- **Do not purchase from third-party websites**. Although these sites may seem trustworthy and offer good deals, they often exist to trick users into initiating false transactions for in-game assets they will never actually receive.

For all non-Veteran Affairs related fraud, reach out to the Federal Trade Commission (FTC)

Online: https://reportfraud.ftc.gov

For more information please visit www.va.gov/VSAFE

VA | U.S. Department of Veterans Affairs