FORGE

The Arkansas Cyber Defense Center

Online Shopping Scam

An online shopping scam involves a scammer who uses the internet to trick you into buying fake or counterfeit items.

Why be aware of this scam?

This scam can be easy to fall for. Scammers will often create websites or create social media accounts that look legitimate. Often, the scammer will take your money, and never send any kind of product.

Red flags:

- Sketchy looking website with typos and poor grammar
- Asking for personal information before you purchase (email address, SSN, birthdate, etc.)
- No contact information
- Prices set way lower than everybody else
- No confirmation email after purchase
- Redirected to a different site for checkout

Immediate action:

- If you have already provided your financial information, contact your financial institution to see about stopping transactions or canceling accounts.
- If you paid using gift cards or a wire transfer, contact the issuer. They might be able to help you stop the transaction.
- Keep all documentation related to the scam in case you need to file a police report.
- If you provided personal information, like your Social Security number, you may be at risk for identity theft. Contact your bank or credit card company to make them aware. Then, contact the three major credit reporting agencies – Experian, TransUnion and Equifax – and place a fraud alert on your credit reports. This will make it harder for the scammer to open new accounts in your name.

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599