Holiday Consumer Alert

PROVIDED BY THE MISSISSIPPI ATTORNEY GENERAL'S OFFICE

The Mississippi Attorney General's Office urges consumers to be aware of scams this holiday season. Scammers take advantage of how many people shop through online platforms during the holidays and often are distracted by all that is going on. Below are scams (both new and old) and tips on how to avoid these scams for the holiday season and new year.

Package Delivery: Be wary of text messages, purporting to be from mail carriers such as USPS, UPS, and FedEx. While the message looks like a legitimate tracking notification with a valid tracking link, it may be a scam. The clickable tracking link can either install malware on your device or bring the user to a form to enter personal information in order to receive a non-existent package. Mail carriers will never send you unsolicited messages when you have not signed up for tracking of a recent package. Rather than click on a link in an unexpected message, contact the mail carrier through their website or a phone number listed on their site. Also, look for spelling errors in the message and slight changes in the spelling of the carrier company in the link such as "**fed-ex.com**" or "**fedx.com**". If you are expecting a package, keep a record of the tracking number so that a scammer can't trick you with a fake tracking number.

Sham Websites: Watch out for fake websites from illegitimate companies. Make sure the URL in your browser address bar is "**https://**" which indicates that a website is secure. If you are on a website and receive a pop-up message or email asking for your financial information, then this website is not legitimate. Companies will never ask for payment information this way. Other red flags include spelling errors and poor-quality photos.

High-Demand Items: Be careful when buying high-demand items, such as new gaming consoles, this holiday season. Gaming consoles like the new PS5 and Xbox Series X are difficult to find, and scammers have taken advantage of its popularity. Always make sure the website you are buying from is reputable by researching the company thoroughly. Check the item's price from a major retailer, and if you see an item listed at a price much lower than its retail price, this is likely a scam. Watch out for scammers on social media marketplaces or advertisement websites promoting a high-demand item. If someone asks for you to pay for an item with a gift card, it is most likely a scam.

Illegitimate Charities: Scammers may create websites and ask for donations via a legitimate financial tool (such as PayPal) for a non-existent charity. They may also mimic a legitimate charity. Most established charities have registered with the Secretary of State's Office, and the Secretary of State's website will have their address and contact information.

Holiday Consumer Alert

PROVIDED BY THE MISSISSIPPI ATTORNEY GENERAL'S OFFICE

Social Security: It can be intimidating when a caller purports to be a government official; however, consumers should know that the Social Security Administration (SSA) will rarely call you. Generally, you will not receive a call from the SSA unless you've already contacted the agency. Scammers have been known to make your Caller ID show a different number than the number that is actually calling you and sometimes scammers have even called from a spoofed SSA number. If you get a call from the SSA's number and you're worried about your SSN, hang up the phone and call the phone number from the SSA's website. The SSA will never demand payment and will never threaten you with deactivation of your SSN number or with legal action/arrest. The SSA will never call you and tell you your SSN has been suspended because it's been involved in a crime or because it's been associated with fraudulent activity. If you do fall victim to fraud, never be embarrassed to report the in-cident to our office. Every day scammers are adapting and finding innovative ways to appear genuine in order to defraud consumers. If you have a question for a consumer mediator or would like to fill out a complaint regarding a potential scam, you can contact us on our website. **You can also contact us with a general inquiry.**

Heartstrings: Scammers try to build trust through online dating apps or social media apps. Scammers will usually message you from a fake profile and tell you a story that always ends with them "needing money". Stories include money needed to pay for international travel or medical expenses. Never send money to someone you haven't met in person.

Gift Cards: No legitimate business or government agency will ever ask for payment in the form of gift cards. If you've bought gift cards in a scam, alert the company who issued the cards immediately. It's extremely difficult to get your money back because gift cards are basically cash. If you give the scammer your gift card number and PIN, the money is gone unless the company can be contacted without delay.

Online Marketplace: Always check the seller's reviews and be sure the seller includes contact information. Don't pay with wire transfers, gift cards, or cryptocurrency. Scammers use these payment methods because it's very difficult to get your money back. Make sure the payment method is safe and secure, like a credit card payment, which offers protections in case something goes wrong. If a price sounds too good to be true, it probably is.

Tech Support: A caller claiming to be a computer technician from a reputable company informs you that you have a virus on your computer, and it needs new antivirus software. This is a scam! A legitimate company will never contact you and tell you there is an issue with your computer. Also, be wary of pop-ups that resemble error messages from your operating system or antivirus software. These messages often come with a phone number to call. Security pop-up warnings on your computer will never tell you to call a phone number.

The Mississippi Attorney General's Office wishes you a safe and happy holiday season.