Holiday Scams

Beware package notices : Most sites will update you with package shipping and delivery information, but beware if they reach out to ask for your credentials to check on your package. An email with a link to click that goes straight to the UPS or FedEx websites is fine. (Be careful of links that go to some other site). You're always better off going to the shipping site yourself and typing in the tracking number.

Phone facts : Your bank will **never** call and ask you to give them your account information. But scammers do. They call pretending to be a "security agent" or an IRS agent and say that your account's been compromised. To fix it, they ask you to provide them with personal information, often including the account password or a credit card number. Don't give it to them. Call your bank directly (not on a number they give you) and ask them to confirm.

Free Wi-Fi: It's tempting to make use of free Wi-Fi when you're out and about, but be cautious. Sometimes it's the store but sometimes it's cybercriminals providing the service. When in doubt, check and make sure the Wi-Fi really is set up by the business you're in.

Check your card: If you can, use one credit card for all your online purchases, so you can easily see if there are charges for items you didn't buy. You'd be surprised how many people don't actually go through their credit card statement each month. January and February are the months to do it, as any unscrupulous charges will show up on those bills. You can't dispute a charge if you didn't notice it was there, so check your statement.

Passwords: Yes, we know changing your passwords is a hassle. You should change them before and after the holidays, in case it turns out that one of the sites you shopped on was compromised. This will assist in protecting your account.

Chancy Charities : Many organizations make a pitch for end-of-year giving around now. Scammers know this and send out emails from fictitious groups to hop on the bandwagon. Do your homework. Check the group's website as well as sites such as Charity Navigator, Charity Watch and the BBB Wide Giving Alliance to confirm it's for real.

Digital delights : Electronic holiday cards are increasingly popular. But if you send them, make sure you choose a well-known site. Scammers sometimes set up malware-ridden sites that can infect not only your computer, but the computers of the friends and family you send to.

iScams: New mobile apps for Android and iOS devices are added every day. Thanks to the ongoing advancement of technology, your mobile device can control the temperature in your house, keep you connected to social media, and add cool filters to your holiday photos. Even the most official-looking or festive apps could be malicious and capable of accessing your personal information. McAfee Labs™ recently found a suspicious Android app called “ACCLeaker” that secretly collects a device user’s Google account ID, Facebook account ID, and Twitter account name.
TIP: Google and Apple have made tremendous efforts to scan apps uploaded to their app stores, so you should only download apps from these official app stores. Pay attention to how much information an app requests and, if the app requests too many permissions, do not download it. It may be requesting access to information on your phone that you would prefer to keep private or more information than it needs. Also install antivirus software on your mobile device to help protect against malware getting on the device.

Gift Cards : Scammers will go to racks of gift cards, and using handheld scanners, read the code on the magnetic strip of the card and the number on the front. They put the card back on the display and periodically check with the retailer by calling the 800 number to check whether the card has been activated**.** Shortly after,

they attempt to use the card online or in person. Buy gift cards which have been properly secured.

Please call the Winfield Police Department with any questions or concerns. 630-933-7160