O'Fallon Police

Neighborhood Watch Newsletter – December 2020

Christmas Tree Fire Safety

If your holiday isn't complete without a live Christmas tree, follow these safety precautions to reduce the risk of fire.

• Fresh trees are less likely to catch fire, so look for a tree with vibrant green needles that are hard to pluck and don't break easily from its branches. The tree shouldn't be shedding its needles readily.
• Always place your tree away from heat sources like fireplaces, radiators, candles, heat vents or lights, and keep the tree base filled with water to avoid a dry out.
• Make sure all your indoor and outdoor Christmas lights have been tested in a lab by the UL or ETL/ITSNA for safety and throw out any damaged lights.
• Any lights you use outdoors must be labeled suitable for exterior placement and be sure to plug them into a ground-fault circuit interrupter protected receptacle.
• Keep all your holiday candles away from your Christmas tree, surrounding furniture and décor.
• Bedtime means lights off! Don't forget to turn your Christmas tree lights off each night.

Protect Yourself From Package Thieves

December is the busiest month for online shopping and home deliveries. Protect yourself from *"porch pirates"* with these package delivery tips.

- Consider having your packages **delivered to your workplace** if your employer allows it.
- **Track your package** so you know when it has been delivered.
- **Team up with your neighbors** to watch for suspicious activity or bring packages inside if you aren't home.
- Consider installing home **security cameras** and register them with OPD so we can contact you to check your footage if a crime is reported near you.

Unfortunately, Breakfast with Santa will not be held this year but the O'Fallon Police Department will still be a collection site for the US Marine Corps Toys for Tots Program. If you would like to donate a **new, unwrapped toy** please bring it to the O'Fallon Police Department main lobby between now and **December 10**. Donation boxes are located by the Records window.

For more information, contact Detective Adam Krack at akrack@ofallon.org

Protect Yourself from "Crimes of Opportunity"

Cold weather means cold cars in the morning. You aren't the only one who doesn't like getting into a frigid vehicle on a winter morning; neither to THIEVES! Auto Theft is on the rise in the St. Louis area and O'Fallon is no exception. While it's tempting to warm your car for a few minutes while you get ready in the morning, this is just the opportunity car thieves are looking for.

If you don't have access to a warm and secure garage and need to warm your car, consider installing a remote starter that will run the engine for a short time but won't allow the vehicle to be driven away. Don't give your car to a thief!

United States Secret Service Cybercrime Investigations

Consumer Tips for Secure Online Shopping 2020 Holiday Season

U.S. retail e-commerce sales are expected to explode this holiday season. With the ongoing COVID-19 pandemic changing shopping behaviors, retail online sales are predicted to increase by 25%-35% over last year's holiday season sales and generate up to $196 billion. With that much predicted revenue, the risk of online fraud increases exponentially. Online criminals will be stepping up their efforts to prey upon unsuspecting or unprepared consumers. The U.S. Secret Service would like to remind you to stay vigilant and provide you with the following information and best practices to achieve a more secure online shopping experience this holiday season.

Software and Antivirus Updates: Install operating system and antivirus definition updates as soon as they are available for all devices you use for shopping, to help protect yourself online.

Account Passwords: Change passwords to online shopping sites and other accounts regularly, and use different passwords for each system and account. Utilize multi-factor authentication for an added layer of login security, when available. Immediately change factory preset passwords on home networking equipment, such as Wi-Fi routers and smart devices.

Payment Cards: Credit cards have better protections for the consumer if fraud occurs. For more information, visit the Federal Trade Commission (FTC) Consumer Information. Verify online transactions by checking your credit card and banking statements routinely.

Public Wi-Fi: Do not conduct online shopping or banking using publicly available Wi-Fi networks. While the network in a restaurant, coffee shop or store may require a password, there is no guarantee as to how secure the network is, or who may be monitoring and intercepting your online transactions.

Phishing and Smishing: Phishing (email) and Smishing (text message) are types of fraud schemes which criminals use to elicit funds, credit card and personally identifiable information (PII), or install malware on computers and electronic devices. Never respond to emails or text messages from unknown sources, and avoid opening attachments or clicking on links from senders you do not recognize. Often, these attachments or links can contain malicious content that can infect your device or computer and steal your information.

Social Engineering: Be wary of emails or calls asking you to provide your PII information such as your login, password, account number, etc. Legitimate businesses and government agencies will never solicit personal information by sending you an email, text message, or calling you. Utilize the customer service numbers on your credit/debit cards/bank statements or the merchant websites to verify any requests for information.

Online Transactions: Reputable and established online businesses utilize encryption, such as TLS/SSL security, to protect your PII and payment information as it is transmitted to and from your computer or device. SSL/TLS are protocols for establishing authenticated and encrypted links between networked computers. To protect your information, look for the Lock icon next to a website address in your browser. Do not ignore certificate error notifications, they can be a warning sign that you may be visiting a fraudulent or "spoofed" website. A website's certificate provides identification of the web server. If the certificate has an error, it might indicate that your connection has been intercepted or that the web server is misrepresenting its identity. Always verify website addresses by manually typing them in the browser, or access websites from internet searches. When shopping from your phone, only consider vetted apps from trusted businesses and download only from the device designated app store.

Remember, if the offer sounds too good to be true, then it probably is.

For more information, visit https://www.secretservice.gov/investigation/

United States Secret Service Cybercrime Investigations

Merchant Tips for Securing Your Online Payment Platform 2020 Holiday Season

U.S. retail e-commerce sales are expected to explode this holiday season. With the ongoing COVID-19 pandemic changing shopping behaviors, retail online sales are predicted to increase by 25%-35% over last year's holiday season sales and generate up to $196 billion. With that much predicted revenue, the risk of online fraud increases exponentially. Online criminals will be stepping up their efforts to prey upon merchants' unsecured or outdated payment platforms. The U.S. Secret Service would like to remind you to stay vigilant and provide you with the following information and best practices to achieve a more secure online shopping experience this holiday season.

Software and Antivirus Updates: Install operating system and network software patches, firmware updates, and antivirus definitions as soon as they are available. Discontinue the use of outdated, unsupported operating systems.

Account Passwords: Immediately change factory preset passwords, change passwords regularly, and use different passwords for each system and account. Utilize multi-factor authentication and offer multi-factor authentication to customers.

Network Segmentation: Segregate payment system processing from other network applications, proper network segmentation and segregation lessens the network exposure.

Firewalls, Intrusion Prevention and Detection Systems: Use firewalls, properly configure and monitor intrusion prevention and detection systems for added defense.

Remote Access: Limit network remote access when and where possible. Always secure remote access and monitor for unusual activity to reduce risk. Identify a baseline of remote accessactivity for reference.

Backups: Have cold storage backups and test restoration of backup files regularly.

Online Payments: Utilize Payment Card Industry Data Security Standards (PCI DSS) for online transactions, to include encrypting (SSL encryption) customer PCI data being stored, processed, or transmitted. Verify card holder address and require Card Verification Value (CVV) code to help authenticate and validate card holder information.

Monitor: Implement software code integrity checks by scanning the payment website for irregularities within the software code (JavaScript). Monitor and analyze web logs.

e-Skimming: The Silent Threat Lurking in Your Payment Platform

What is e-Skimming

Cybercriminals introduce malicious code on e-commerce payment card processing web pages with the intent to capture personally identifiable information (PII) and payment card industry (PCI) data. The malicious code is introduced through exploiting vulnerabilities on website e-commerce platforms or by gaining access to their network through third-party vendors who provide advertisements and web analytics on payment processing platforms. The captured data is then sent to domains under the cybercriminal's control.

How to Mitigate it

Malicious code signatures known to law enforcement are highly variable and are increasingly difficult to detect. Besides the best practices information listed above, continually monitor your payment website for software code changes. Implement software code integrity checks by scanning the payment website for irregularities within the software code (JavaScript). Monitor and analyze the associated web logs.

For more information, visit https://www.secretservice.gov/investigation/

RESTORE ILLINOIS

Tier 3 Resurgence Mitigations

OPEN

- **BARS AND RESTAURANTS** — OUTDOOR SERVICE, PICKUP & DELIVERY
- **CRITICAL INFRASTRUCTURE AND TRADES**
- **GROCERY** — AT 50% CAPACITY
- **HEALTH AND FITNESS CENTERS** — AT 25% CAPACITY
- **HOTELS** — LIMITED TO REGISTERED GUESTS
- **MANUFACTURING** — WITH SAFETY GUIDELINES
- **OUTDOOR SPORTS & RECREATION** — WITH 10 PERSON GATHERING LIMITS
- **PERSONAL CARE SERVICE** — AT 25% CAPACITY
- **PHARMACY** — AT 50% CAPACITY
- **RETAIL** — AT 25% CAPACITY
- **SCHOOLS AND DAY CARE** — (LOCAL DECISION)

PAUSE

- **BANQUET HALLS & EVENT SPACES**
- **CULTURAL INSTITUTIONS**
- **GAMING AND CASINOS**
- **INDOOR FITNESS CLASSES**
- **INDOOR GROUP SPORTS & RECREATIONAL ACTIVITIES**
- **OFFICES SHOULD WORK REMOTELY IF POSSIBLE**
- **LIMIT GATHERINGS TO YOUR HOUSEHOLD**

For more detailed information, visit https://dceoresources-ss-assets.s3.us-east-2.amazonaws.com/public/Restore-Illinois/Tier-3-COVID-19-Resurgence-Mitigations.pdf