COLORADO
Department of Public Safety

Preventing Motor Vehicle Theft

Best Practices Guide for Auto Dealerships

April, 2024

Authored by:
Trooper Jason McCall, CPP, PSP, ABCP
Colorado Department of Public Safety

COLORADO
Department of Public Safety

Investigative Services Section, ISS

Beat Auto Theft Through Law Enforcement, BATTLE

In partnership with:

CIAC
Colorado Information Analysis Center
Department of Public Safety

Division of Homeland Security & Emergency Management
Office of Prevention and Security

Introduction:

This report was developed through a collaborative effort that included significant contributions from the Colorado State Patrol's Beat Auto Theft Through Law Enforcement (BATTLE) program, the Auto Theft Intelligence Coordination Center (ATICC), the Colorado Information Analysis Center (CIAC), the Colorado Auto Theft Prevention Authority (CATPA), local law enforcement, and numerous private sector partners and dealership representatives. The intention of this guide is to support security planning efforts and complement existing programs. This report was developed based on information discovered during a limited research project and should not be considered an exhaustive list of security measures or best practices.

If additional resources, information, or guidance are needed, please reach out to the Colorado State Patrol's Investigative Services Section. Support could include assistance with program implementation, policy and procedures, resource allocation (i.e. prioritization), and general questions or guidance.

This report contains sensitive information intended to offer protective measure options for consideration for the automotive dealership industry. Please consider using discretion regarding the circulation, sharing, reproduction, and dissemination of this information.

Purpose:

Identify, establish, and share industry best practices and lessons learned to mitigate occurrences of auto theft among Colorado auto dealerships and auto rental facilities.

Methods:

Our team conducted unstructured site assessments, met with dealership management and personnel, auto theft investigators, crime analysts, and reviewed auto theft intelligence data spanning from January 2017 through April 2022 (referred to as the *data research period*). We analyzed data from dealerships with the most reported cases of auto theft and data from dealerships with the least reported cases during the data research period to consider potential contributing and mitigating factors. This cross-sample analysis consisted of regionally and operationally diverse locations, including rural, metropolitan, large dealerships, and small dealerships. Additionally, as available, we assessed the methods and tactics used to complete the crimes and researched prevention options.

Protective measure investments may be thought of in terms of the deter, detect, delay, defend paradigm and should be supported by written policies when practical. The primary goal should be to make the facility a less attractive target in order to deter undesirable activity. If a bad actor does target the facility, then protective measures should enable personnel to detect the activity before harm is done, delay an imminent act, or if no other measure is successful, then defend against the act.

As we evaluated options for consideration (i.e. recommendations or best practices), we examined and prioritized free, no-cost, and low-cost solutions. As a result, we provided several resources to consider; however, we encourage organizations to conduct their own research to determine the best solutions for each situation, budget, needs, and application.

Considerations:

Technology alone should **not** be expected to completely mitigate an identified problem (e.g. cameras do not necessarily prevent bank robberies but are intended to provide forensic information that supports an investigation). Additionally, a key lockbox is a best practice we include in the following report; however, if the organizational culture allows for keys to be left unsecured on a desk, the lockbox is not a sufficient security control. Therefore, all security controls and measures should be supported by checks and balances (i.e. policies and procedures).

As an added guide to assist with making decisions regarding protective measures, we identified threats that most often occur during business hours and may require different protective measures when compared to threats occurring after hours. For convenience, we have included icons to indicate the business model may be adjusted to address threats during business hours versus threats occurring after hours.

☀ ☾

Additionally, there may be options available and/or best practices we were not aware of during the creation of this guide, and we welcome suggestions, comments, and input. We have put our best effort into providing accurate information in the development of this Best Practices Guide, but we realize technology, tactics, methods, criminal intelligence, etc., may evolve, resulting in a need to reappraise best practices over time.

Executive Summary Table:

The table below summarizes our findings related to themes, tactics, and resources often used to facilitate auto theft from dealerships and mitigate the threat or impact. Additional details are provided in individual sections that expound on each topic. Related links are contained within each theme in this table that will take the reader to the associated page for more information.

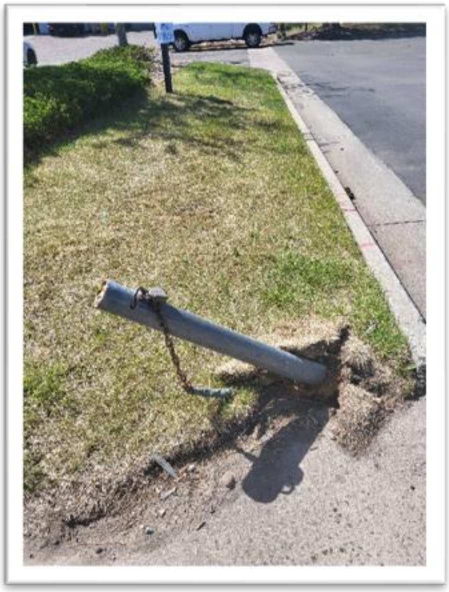
Theme	Tactic	Option to Consider
Smash-and-Grab (pg. 5-7)	Use ramming vehicles to push blocker vehicles away from property entrances, force open garage doors (service bays, etc.), and break glass windows. Once subjects gain access to the building, keys are stolen.	Layered defense: fencing, bollards, cable, environmental design (i.e. large rocks, trees) around the perimeter (see CPTED). Park large vehicles inside garage entries against bay doors (see pg. 7), and add security films to the glass (laminated glass). Key control measures (several best practices available depending on circumstances).
Fraudulent Identification (pg. 8)	Provide false identification (ID) to defraud the purchase process.	Compare the signature on the ID to the signature provided on a test-drive document. Collecting a physical or digital fingerprint may deter criminal actors and can assist law enforcement with identification.
Key Swap (pg. 9)	Swap OEM key with decoy to facilitate theft at a later time.	Use anti-tamper key tags. Dealership employees can maintain control of the keys at all times.
Defeat or spoof OEM GPS (pg. 10)	Damage or remove antennas or other components.	No-cost (to dealership) GPS that can be hidden and offers shareable tracking and lot management: https://www.recovr.biz/co.
High-Tech Theft (pg. 11)	Access the OBD module to program, reprogram, or clone the key signal.	Lock OBD port* or install kill switch. Utilize Faraday containers. Approximately $29 (at the time of writing)
General Crime (Cat theft, drilling gas tanks) (pg. 11)	Walk on-premises, use battery-powered tools.	Cameras with two-way communication and analytics, lighting, Crime Prevention Through Environmental Design (CPTED).
Investigative Considerations (Appendix)	(Additional considerations)	Consider configuring wi-fi router settings to protect networks and capture guest connection information to support criminal investigation.
General Security Planning (Appendix)	Internal vs. external threat, threat levels, communications, lighting, etc.	Deter, detect, delay, defend paradigm, layered defense.

*It should be noted the State does not endorse any specific vendor. Any products or services referenced are for informational purposes only, as there are many vendors that may provide these or similar solutions.

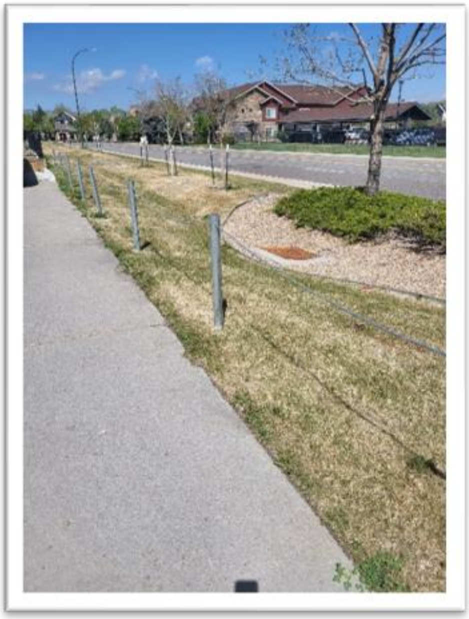
Smash-and-Grab (forced entry)

History: Vehicles have been used to force entry through chains, inadequately secured barriers, gates, and push past vehicles positioned at dealership parking lot entrances intended to control access to the parking lot.

Challenge: Channeling is likely not an option for sites that do not have secured perimeters (i.e. open lots). Bad actors have demonstrated a willingness to disregard landscaping, curbs, signs, etc., and exploit soft boundaries to gain access to dealership lots. Inadequate and/or unused key storage leaves keys vulnerable to theft.

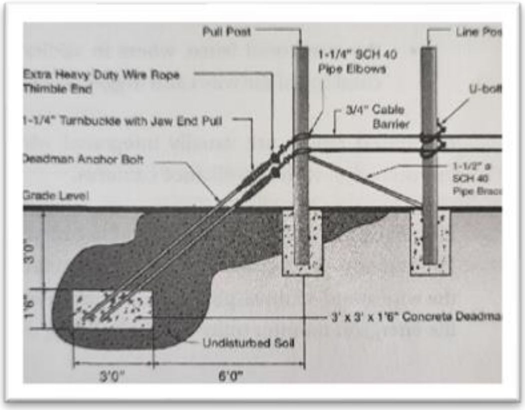


Options for Consideration:



Channel vehicles through driveway access points. Large rocks/boulders, fencing, rails, and perimeter safety cable strung through adequately anchored solid-core posts may reduce this vulnerability.

(*Consider referencing federal, state, and local requirements, and/or life safety codes prior to implementation of protective measures)



Department of Defense, 1999

(For more information regarding security design elements and strategy, see Crime Prevention Through Environmental Design (CPTED) in the Appendix.)

Removable impact-rated bollards can be used to secure driveways after-hours (Figure 1, permanent bollard shown to illustrate installation best practices).

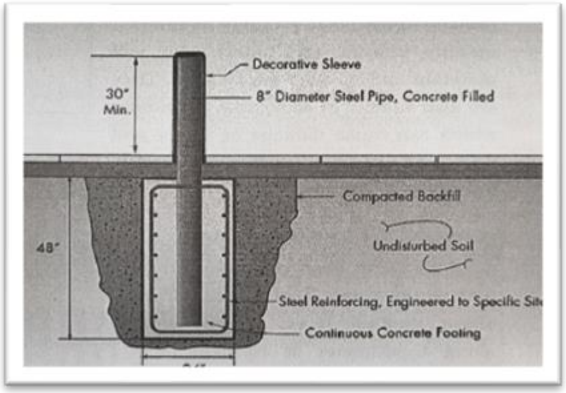
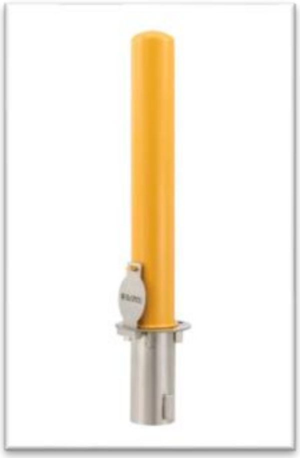

Decorative Sleeve
8" Diameter Steel Pipe, Concrete Filled
30" Min.
Compacted Backfill
Undisturbed Soil
48"
Steel Reinforcing, Engineered to Specific Sit
Continuous Concrete Footing

Figure 1, U.S. Department of State



Although, more cost-effective than other options, hollow fence tubing will likely not prevent a vehicle from being used to force entry past this type of barrier.

Metal posts (e.g. >4” diameter), properly anchored at multiple points and spaced less than 8’ apart, are a best practice.

Forced Entry at Service Bay ☾

History: Ramming vehicles may be used to force access into service bays (i.e. garage doors). Once inside the building, subjects are often able to steal keys that may be readily available within the Service Department and offices, as well as keys contained within key storage containers (low/no-security containers such as file cabinets).

Challenge: Roll-down style doors provide little security protection against vehicle ramming attacks. Additionally, alarms do not necessarily prevent this attack method but could contribute to reducing the time an individual spends inside the otherwise secured space.

Option for Consideration: Consider positioning a vehicle across the door width on the exterior (Figure 2) in a front-to-back configuration, to reduce the likelihood of vehicles being pushed out of the way.

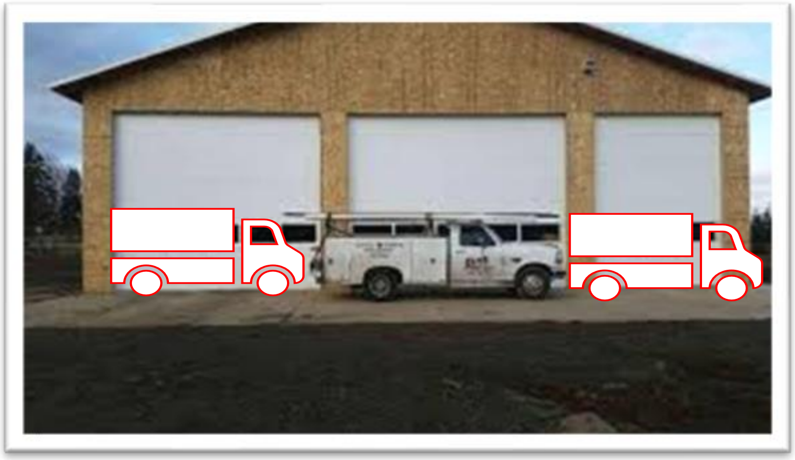


Figure 2 **Park large vehicles in front of bay doors**

A best practice recommendation to reduce vulnerabilities associated with bay doors is to position large vehicles directly in front of the doors, ideally, on both sides.

Park large vehicles in front of bay doors

Security Key-Management Options for Consideration ☀ ☾

Security key management system
http://www.1micro.com

Numerous security key management systems exist on the market. These devices should be secured in place, housed in a secure area/room, not be visible from public spaces, and be constructed to industry-certified standards, such as ISO/TC332. Additionally, some dealerships may find that removing the keys from the property after hours is a viable option or alternative to securing keys on the premises.

These are not security rated locks

Some key storage devices we observed were equipped with easily defeated locks, such as tubular locks or locks containing standardized pin patterns. These locks and associated keys are avai.lable for purchase online, and replacement keys are available and standardized.

Cabinet lock with standard key and pin pattern

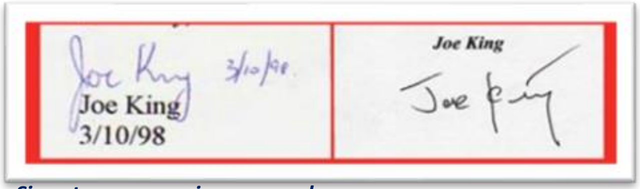
Tubular lock

Fraudulent Identification ☀

History: Subjects provide various forms of identification and information as requested by the dealership to facilitate a transaction (i.e. purchase, test drive, etc.)

Challenge: Dealerships may not have a mechanism or process for validating or authenticating the identification of the individual.

Option for Consideration: Compare the signature on the ID to a signature provided on a test-drive document at the time of the visit. Consider maintaining a copy of these documents until the transaction has been completed and cleared by financial institutions.


Joe King
3/10/98
Joe King
3/10/98
Joe King
Joe King

Signature comparison example

Digital finger print scanner

Although more intensive, obtaining a physical or digital fingerprint may act as a deterrent to would-be criminals and assist law enforcement with identification. Various technologies and options are available.

Inkless finger print pad

Key Swap ☀

History: The subject is provided the OEM vehicle key during the test drive and swaps the key with a blank/decoy key. The subject(s) return and use the previously swapped key to steal the vehicle.

Tamper resistant tag

Challenge: Personnel shortages may restrict the opportunity to have an employee accompany customers during test drives and maintain control of keys.

Option for Consideration: Employees should maintain control of keys and/or utilize tamper-resistant tags to reduce the likelihood of a swap. Sequentially numbered anti-tamper tags that are recorded in a log are ideal (e.g. tag #002103, 2012 Honda, VIN#...)

GPS-Related challenges ☀ ☽

(e.g. not equipped, defeated, registration lag, etc.)

*Although this theme relates to recovery and not necessarily to preventing auto theft, improved recovery statistics may lead to reduced targeting of dealership assets.

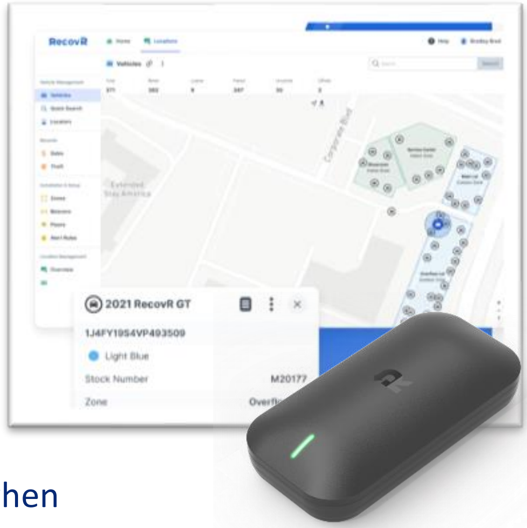
UNDER NO CIRCUMSTANCES SHOULD SOMEONE OTHER THAN LAW ENFORCEMENT ATTEMPT TO LOCATE OR CONTACT A STOLEN VEHICLE.

History: High-target vehicles, often preowned vehicles and including rental vehicles, may not be equipped with active GPS devices. Intelligence suggests criminals remove and/or damage factory-installed GPS system components, such as the antenna, interfering with recovery attempts.

Challenge: It may be cost-prohibitive to equip the entirety of a large inventory or highly-targeted preowned vehicles with expensive tracking devices. Dealerships may be relying on factory-installed GPS systems to recover inventory. These factory-installed devices have limited effectiveness, as demonstrated in Colorado vehicle theft cases due to gaps in device activation (i.e. the time delay between delivery and "received as inventory"), and delays in real-time GPS location.

Option for Consideration: Install an aftermarket, battery-powered GPS device away from the area immediately around the dashboard (i.e. not in or behind the glove box, or behind the radio). Devices hidden in and around the glove box or radio are more likely to be discovered. RecovR brand vehicle theft recovery system is a no-cost option for dealerships.

Benefits: Zero upfront costs to dealerships, 5-year battery life, can be leveraged as a free lot-management tool, provides real-time location of inventory and notifications when vehicles move beyond predetermined areas.



2021 RecovR GT

1J4FY19S4VP493509

Light Blue

Stock Number M20177

Zone Overfl

RecovR GPS device and lot management shown

From a recovery perspective, the ability to share a link with responding law enforcement officers streamlines recovery and allows for real-time tracking of vehicles from a mobile device or computer.

High-Tech Theft

History: Subjects utilize technology, equipment, and devices to gain access to locked vehicles and bypass ignition security features. Once inside a vehicle, the onboard diagnostic port (OBD port) is exploited and facilitates unauthorized reproduction and/or programming/reprogramming of vehicle keys.

OBD Port Lock

Challenge: These ports are easily accessible and are often used during vehicle maintenance. Criminals exploit locksmiths and other retail organizations and obtain technology otherwise intended for legitimate vehicle service requirements.

Option for Consideration: Install an **OBD Port lock** or an ignition kill switch.

Additionally, some vehicle makes and models are more vulnerable to technical attacks. Ensure manufacturer technology updates (software or firmware) are completed, specifically on vehicles most vulnerable to these types of attacks.

General Crime

History: In order to help deter threats from occurring, one of the primary goals of a security plan should include improving the overall security posture of a facility. During our assessments, we learned of instances involving catalytic converter theft, drilling of gas tanks, and placement of Apple Air Tags (suspected to help facilitate theft off-site or at a later time).

Challenge: These crimes are often unpredictable and occur without notice.

Ring camera and notification shown on cell phone

Option for Consideration: The focus for addressing this theme should be on controls that deter and detect these types of attacks. One successful example we identified included the use of video cameras equipped with alert notifications and 2-way communication capabilities. When an alert is received, live verbal communication with the subject(s) has resulted in scaring off would-be criminals. Technology and service range from 24/7 staffed security operations with live monitoring to selfinstalled and managed Ring camera systems. We recommend wired cameras over wireless.

Please keep in mind that cameras are often installed in locations that reduce the likelihood of vandalism to the device, resulting in camera views from elevated positions/angles. This results in capturing images that provide limited forensic value (i.e. observation of an individual) rather than identification (i.e. facial features). Systems not coupled with live notifications provide little to no security-related preventative value.

Appendix

General Security Planning

Security approach: Although not specific to preventing auto theft, this General Security Planning section is included to help contribute to the overall security posture of an organization and subsequently reduce crime as a whole.

Considerations:

- A layered security approach is used to form concentric circles of protection around identified assets. Create multiple layers, also known as target hardening, to reduce the likelihood of a bad actor gaining access to protected assets. Layers can include security controls such as the options listed above but may also consist of policies and procedures.
- Regarding prioritizing limited resources, the deter, detect, delay, and defend paradigm, should be considered when allocating limited resources.

Insider threats: According to the Cybersecurity and Infrastructure Security Agency, insider threat incidents are possible in any sector or organization. An insider threat is typically a current or former employee, third-party contractor, or business partner. In their present or former role, the person has or had access to an organization's network systems, data, or premises and can continue to use their access for reasons other than for approved business purposes. To combat insider threats, organizations can implement a proactive, prevention-focused mitigation program to detect and identify threats, assess risk, and manage that risk - before an incident occurs. [1]

Full-scope background checks can prevent or deter insider threats. They help establish a baseline of “normal” behavior for each employee that can illuminate key changes over time.

- Recurring checks can be scheduled at regular intervals (e.g. annually) and/or after significant events (e.g. divorce, bankruptcy, etc.)

Lighting: A best practice is to ensure lighting is uniform, overlapping, and promotes observation of personnel at main entrances, parking lots, and building façade areas.

- Ensure landscaping does not interfere with lighting as the seasons change (more information regarding landscaping is provided in the section below titled Property Maintenance.)

Property Maintenance: When practical, maintain a clear buffer zone (i.e. a clear area that provides an opportunity for observation between the perimeter and any buildings or structures that could offer concealment.) Regular attention and maintenance to landscaping may include: pruning of trees (up from the ground to +8 ft.), shrubbery (keep lower than 32 in. high), and vegetation, as well as an awareness of areas that may aid in the concealment of individuals in low lighting areas (shadows), not providing natural observation (e.g. natural observation: an exterior area that has the opportunity to be observed from a window.)

- Consider removing landscape rocks from the property that could be thrown through glass. Alternatively, using concrete to secure the rocks together may be another option to removal.

Access control: A good access control program has:

- Electronic means of assigning hierarchy privileges based on the least access required.
- A provision for inventorying and auditing access.
- Capability to immediately assign or remove an access holder.
- Accountability for any hard keys that remain in the system.
- Door position sensor alarms to deter door-propping.

Communications: Ensure preplanned measures exist that facilitate timely and efficient communication to guests, customers, employees, and organizational leadership during an emergency situation.

- Pre-scripted messages are a best practice and should include information regarding specific scenarios identified as most likely to impact your operations (these should also be listed in an emergency plan).

Information Sharing: Information sharing is a valuable precursor to good security planning and is completely free. Consider establishing a community-based (i.e. area dealership groups) or neighborhood watch-style group that shares safety and security concerns and volunteers to receive intelligence information on behalf of their institution.

Key Management (other than vehicle keys): It is a best practice to maintain records of keys. This should include who holds the keys, check-in/out dates, the level of access the keys afford, and details surrounding lost or stolen keys. Additionally, measures should be implemented to secure keys of sale vehicles and dealership-owned service vehicles (e.g. loaner vehicles and parts delivery vehicles) in the service department.

Signage: Signage can act as a deterrent, provide trespassing notices, and warn of alarm or security camera monitoring.

- Signage indicating policies regarding trespassing, unauthorized/extended stay vehicles, and "Authorized Staff Only" may be considered for use in internal and external areas as appropriate.
    - Ensure policies and procedures exist that support enforcement of violations relating to signs.
- Consider marking all doors, on the inside and outside, to aid in emergency response (e.g. North 1, West 2 for exterior doors, and room number with the corresponding floorplan for interior areas). Exterior facing signs should be visible enough that first responders can see them from a distance (e.g. 50 feet).

Cameras: Cameras, when supplemented with analytics, may allow for significantly improved response to an incident.

- If cameras are not monitored, video analytical software (aka video analytics) can provide immediate notification of violation of a predetermined anomaly (e.g. a person enters a secured area during predefined times resulting in an image notification being sent to a specific group.) Video analytics can be phased in, and deployment priority is given to vulnerable, sensitive, and significant areas and assets (SAAs).
- Consider periodically reviewing historical video footage (i.e. footage that is not live-monitored). Often this can provide insight into otherwise unknown events (e.g. suspicious activity, attack preplanning activities).
- Regular reviews should be performed to ensure these systems are functioning as intended under all environmental conditions (i.e. sunset, night, snow, lack of artificial lighting, etc.)

- Consideration: cameras are often positioned with the intention to reduce opportunities for vandalism to the device. Camera views from elevated positions/angles tend to capture images that provide less forensic value (i.e. observation of an individual) rather than identification (i.e. facial features).

Crime Prevention Through Environmental Design (CPTED)

Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to crime prevention that uses urban and architectural design and the management of built and natural environments. CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants so they can gain territorial control of areas, reduce crime, and minimize fear of crime. CPTED is pronounced 'sep-ted,' and it is also known around the world as Designing Out Crime, defensible space, and other similar terms. [2]

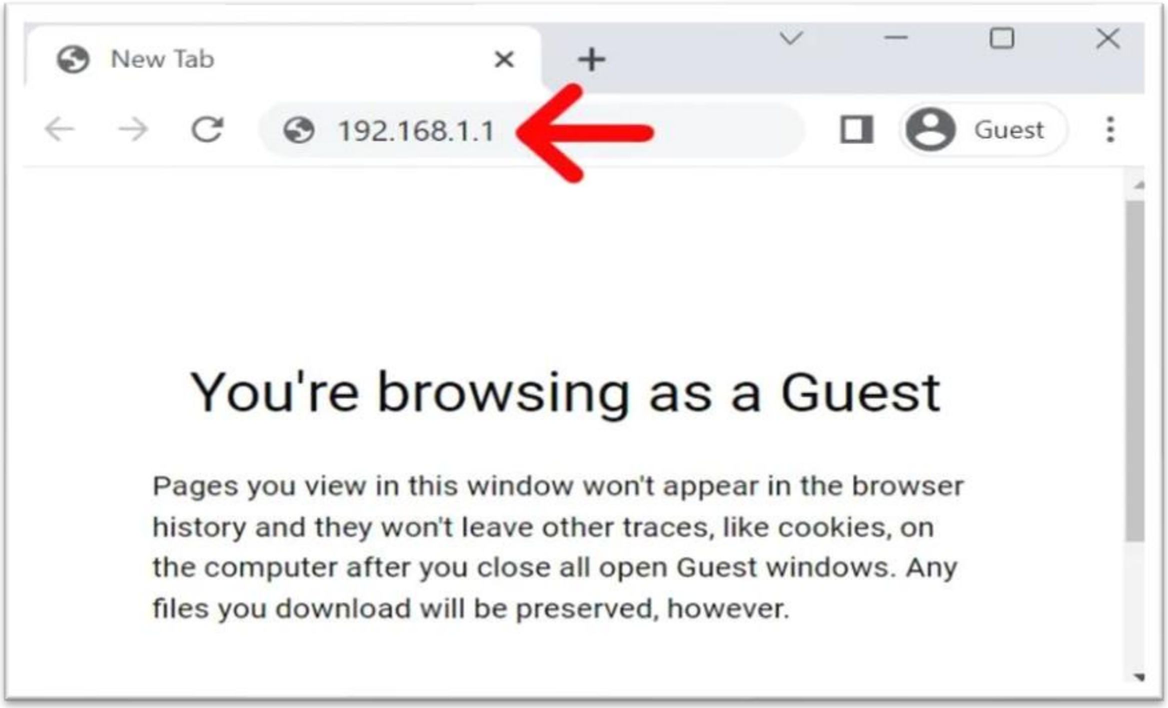
Wi-Fi Guest Network Considerations: [3]

*Consider contacting your network service provider for technical support prior to implementing network changes.

Open Guest networks can provide law enforcement with valuable forensic information regarding digital information of devices within range of networks. Oftentimes, after a criminal event, law enforcement can leverage this potential digital evidence, further advancing the investigation.

Once someone signs into a guest Wi-Fi network (aka virtual SSID), they can access devices and other personal information or potentially expose your network to malware or viruses. In order to protect your network and privacy, we have provided the following steps for setting up a safe guest network:

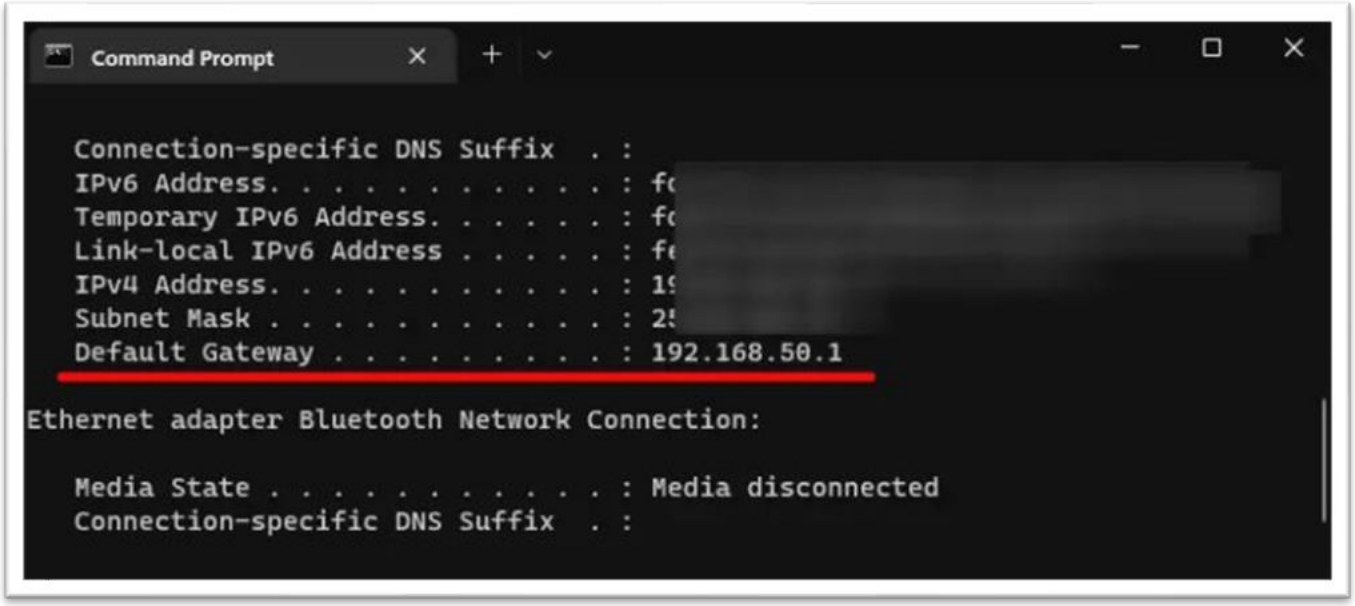
1. Open a web browser (e.g. Chrome, Safari, Edge, etc.)
2. Type your router's IP address into the search bar. In order to log in to set up a guest network, you will need to log into your Wi-Fi router. If you don't know your router's IP address, you can find it with the steps below.



You're browsing as a Guest

Pages you view in this window won't appear in the browser history and they won't leave other traces, like cookies, on the computer after you close all open Guest windows. Any files you download will be preserved, however.

- How to find your router's IP address on Windows: Click the Windows logo at the bottom of your screen or press the Windows key on your keyboard. Then type "command prompt" or "CMD" into the search bar and click enter. Type "ipconfig" into the command prompt window and click enter. You will see your router's IP address next to the Default Gateway.

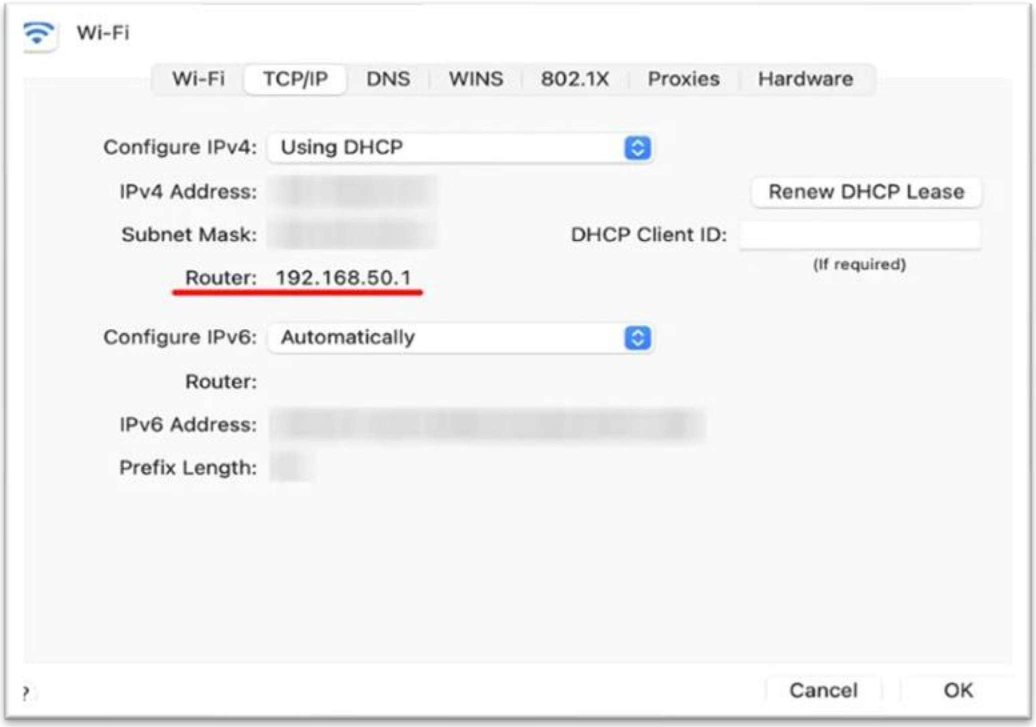


```
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : [redacted]
   Temporary IPv6 Address. . . . . . :
   Link-local IPv6 Address . . . . . :
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . : 192.168.50.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

- How to find your router’s IP address on a Mac: Click the Apple logo in the top-left corner of your screen and select System Preferences. Then click Network, select Wi-Fi in the left sidebar, and click Advanced in the lower-right corner. Finally, open the TCP/IP tab, and you will see your router’s IP address next to Router.



Configure IPv4: Using DHCP

IPv4 Address: [redacted]

Subnet Mask: [redacted]

Router: 192.168.50.1

DHCP Client ID:

(If required)

Configure IPv6: Automatically

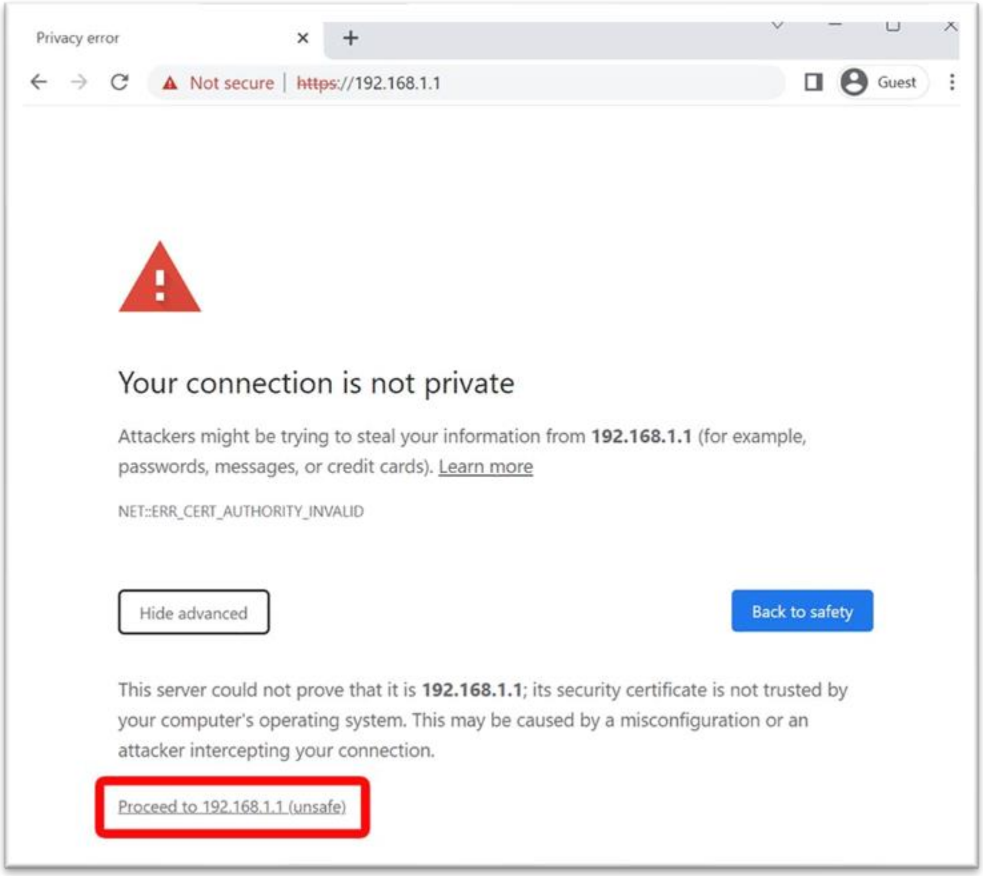
Router:

IPv6 Address: [redacted]

Prefix Length: [redacted]

Re: Warning Message

Note: Once you enter your IP address, you might be prompted that the webpage you are trying to view is not secure. Make sure that you have the correct IP address entered, and then click on the option to proceed. If you don’t see the option, click *Advanced > Proceed*.



Your connection is not private

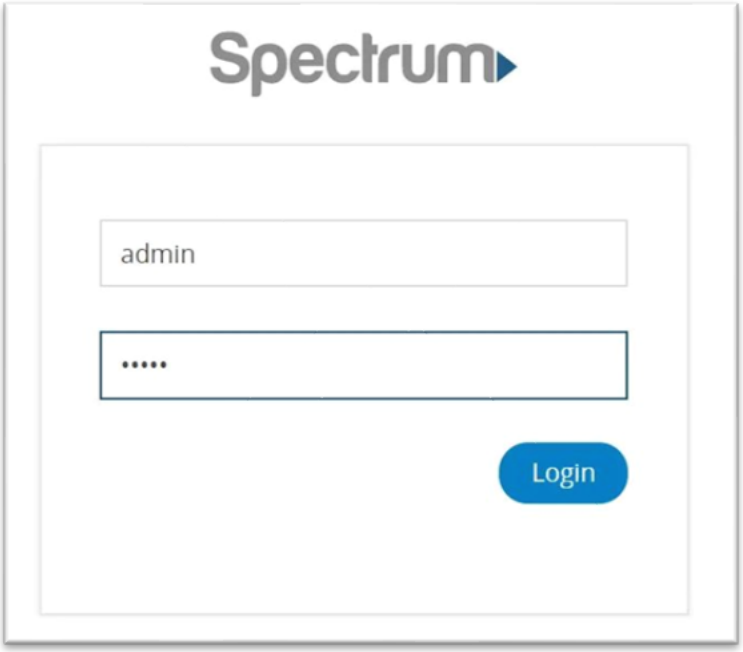
Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.1 (unsafe)

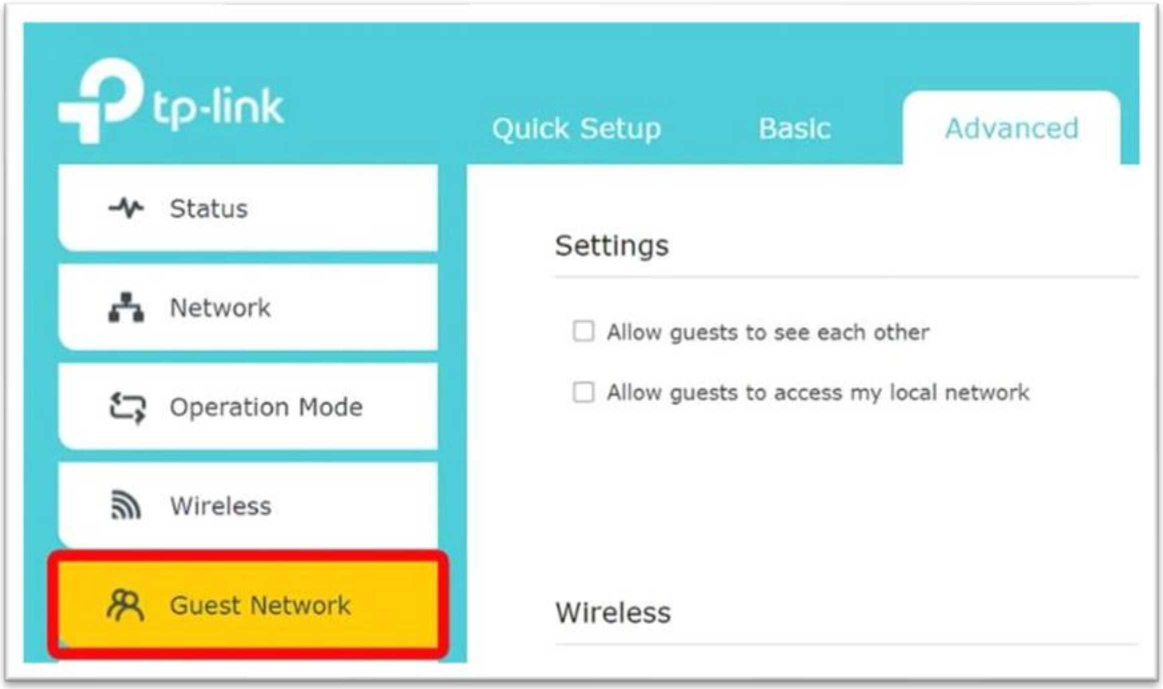
3. Next, enter your router’s login info. In most cases, the default username will be “admin” or left blank, and the password will be “admin,” “password,” or left blank.



admin

•••••

4. Then click Guest Network. If you can't find a guest network button, check under "Wi-Fi," "Wireless Settings," or "Advanced."



Settings

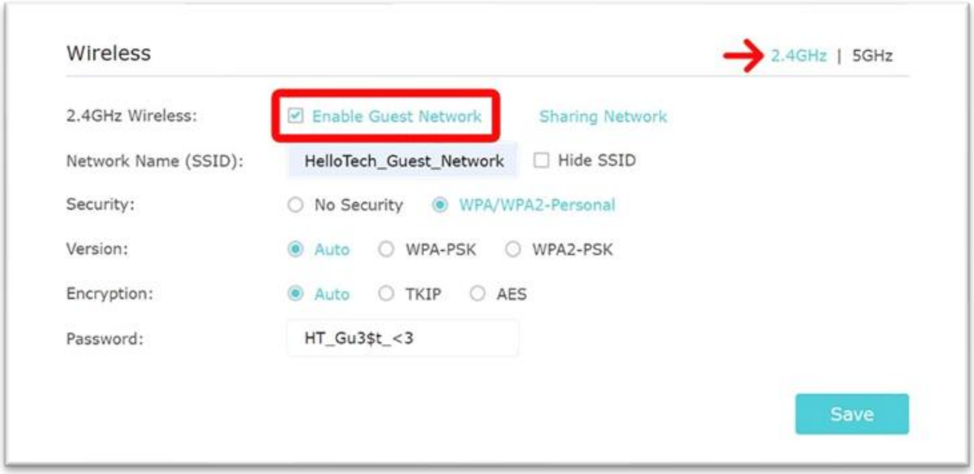
☐ Allow guests to see each other

☐ Allow guests to access my local network

Wireless

Note: There are some routers that do not allow you to create guest Wi-Fi networks. If you do not see a guest network button, check your router's manual online to see if it allows for guest networks to be created.

5. Next, select 2.4GHz or 5GHz and click Enable Guest Network. Depending on your router, you might not see both of these options. The difference between these networks is that the 2.4GHz is slower, but it has a longer range, while the 5GHz network is much faster, but it won't reach quite as far.



Wireless

2.4GHz Wireless: ☑ Enable Guest Network   Sharing Network

Network Name (SSID): HelloTech_Guest_Network   ☐ Hide SSID

Security: ○ No Security   ● WPA/WPA2-Personal

Version: ● Auto   ○ WPA-PSK   ○ WPA2-PSK

Encryption: ● Auto   ○ TKIP   ○ AES

Password: HT_Gu3$t_<3

6. Then you can change the guest Wi-Fi network name and password. The network name is typically labeled “SSID.” Some routers will fill in your network name and password by default, but it is recommended that you change them.

Note: Don’t use the same password for your guest and main networks. You should also choose a password that is easy enough for your guests to remember but hard enough that random strangers can’t guess what it is.

7. Next, choose the guest network’s security settings. Depending on your router, you might have to go to Security settings. If you don’t know which router security option you should choose, check out our guide here.
8. Finally, click Save. You can now share the Wi-Fi name and password with your guests.

Links

security films: https://www.3m.com/3M/en_US/building-window-solutions-us/solutions/

Fingerprint scanners: https://www.bayometric.com/secugen-hamster-pro-20-fingerprint-reader-scanner/

GPS: https://www.recovr.biz/co

Lock OBD port: https://www.amazon.com/Connector-Prevents-Vehicles-Computer-Material/dp/B0BTW92ZPS

key management: https://www.1micro.com

ISO/TC332 : https://www.iso.org/committee/8031077.html

CPTED: Crime Prevention Through Environmental Design: https://www.cpted.net/

Additional CPTED information can be found in the International Standards Organization reference:

ISO 22341:2021 Security and Resilience- Protective Security-Guidelines for crime prevention through environmental design

CATPA Resources

https://lockdownyourcar.org/

References

[1] Cybersecurity and Infrastructure Security Agency, "Insider Threat Mitigation," [Online]. Available: https://www.cisa.gov/insider-threat-mitigation.

[2] T. I. I. C. Association, "CPTED," 1996. [Online]. Available: https://www.cpted.net/.

[3] A. T. I. C. Center, "Assessment of Motor Vehicle Thefts in Colorado 2019," Auto Theft Intelligence Coordination Center , Colorado, 2020.