DESIGN
INSTALL
PROTECT

The burglar's guide to avoiding detection by CCTV

Why it's probably best not to bother because we are going to detect you...

www.ic2cctv.com

Introduction

A brief assessment of internet searches using the AdWords Keyword Planner provided by Google reveals that globally, there might be some interest from people seeking information about how to avoid detection by CCTV. Currently, information on this topic is posted on Google's YouTube as well as many blogs, articles, FAQs and forums.

Using the keyword tool to evaluate a basic selection of terms like 'blind CCTV' and 'jam CCTV', shows there are perhaps up to 500 searches each month, worldwide. The fact is, there is always going to be an interest in such material.

However, the audience is not just those of ill-intent; owners and operators, as well as buyers and those that commission CCTV projects, who may wish to find out about any loopholes and flaws in the technology, are also likely to value this information.

Whatever the motivation, to help those that may be interested in this topic, here we discuss avoiding detection by CCTV surveillance.

Methods of disabling CCTV cameras

Today's CCTV cameras are complex pieces of equipment and there are ways to disable them or interfere with normal operation. To save you the trouble of looking up what these might be, here we briefly outline them.

Blinding cameras

Physical blinding

Where easily accessible, obscuring the lens is the most simple method of making cameras blind. Believe it or not, in one web resource, one way of 'jamming' a camera is to smear jam (or peanut butter!) over the lens to obscure its view. Unsurprisingly, aerosol paint provides the same capability, but should you feel compelled to lick the lens clean, it tastes awful and is quite possibly toxic...

Where cameras are not easily accessible, paintball markers fired from CO2 powered guns are another approach, as is causing physical damage by firing projectiles such as air pellets and crossbow bolts.

Lasers

Laser blinding is where a hand-held laser pointer - of the type popular for presentations - is used to temporarily disable the camera. This is the same practice that has blinded some commercial airline pilots from the ground while in-flight. Lasers of significant power could permanently damage the CCD light sensitive component of a camera.

LEDs

LED lights, such as head torches, may also be effective in preventing identification by creating distortion of the image.

Cyberattack

Hacking cameras

Breaking through poor IT security to gain access to the embedded web servers or other control interfaces enables hackers to interfere with the normal operation or, potentially, hi-jack cameras.

There are known examples where the security of many thousands of cameras and video recorders was breached. The hackers took control and operated them as a botnet (robot network or 'zombie'), and used the collective processing power of the devices to execute computing tasks linked to criminal enterprises.

These include DDoS (Distributed Denial of Service) attacks, which seek to bring down websites to facilitate hacking, and phishing email scams.

Jamming Wireless IP

IP networking is the technology used to transmit images from cameras and send control information to cameras. It uses the same protocol (IP or Internet Protocol) as computer networks, including communication over the web. As well as wired connections, cameras can also be networked over Wi-Fi, or wireless IP.

It is possible to jam Wi-Fi transmit and receive signals with jamming equipment. There are many internet sources of information on making and for buying jamming equipment of different types. Jammers may also be used to interfere with the correct operation of alarm systems, where wireless technology is used by sensors to communicate with the centralised control system.

Defending against attack

While there are a number of methods of interfering with CCTV cameras, the security industry mitigates the risks effectively to preserve the capability to detect intrusion.

In the first instance, many cameras are 'ruggedized' to make them more durable, providing better resistance to physical damage. Filters may be utilised to negate the impact of laser blinding.

Installing them in inaccessible places and eliminating exposed cable runs are basic installation considerations that help to reduce the vulnerability of cameras to physical methods of disablement.

However, someone that truly puts their mind to it is likely to be able to take out a camera. Similarly, a place of business that is targeted by organised criminals with sufficient motivation, such as one holding high value items, may be subjected to a determined cyberattack as part of an attempt to gain physical access.

Hackers with a cause - 'hacktivists', and hobbyist hackers looking to secure bragging rights within their peer groups, may just be intent on stealing nothing but data; however, the fallout from such thefts can be costly in terms of reputation, litigation and compliance failure - just ask the likes of SONY, TalkTalk and Ashley Madison, among many others.

So, how do practitioners optimise system design to reduce the potential for cyber and physical attack to compromise security?

Layered security - a strategic approach

In today's world, where the convergence of security systems with IT continues to evolve, cyber and physical security are of equal importance.

To defend against the exploitation of vulnerabilities which may exist in any one system, to improve protection, security architects and strategists champion the principle of a layered approach. A layered approach means independently operated systems are integrated to work together in concert. This principle applies to both cyberspace and the physical world.

Integrating physical security systems

Integration offers the ability to join up the outputs and control systems of individual security elements at a central monitoring station. This allows for verification of an alert from one system by cross-checking with the outputs of others.

For example, in the case of a camera that has been compromised in some way, the device may send alerts directly to the operators, or smart software analytics may alert that there is no video coming in from it.

This is the trigger for a security response, such as an operative being dispatched to investigate, or another camera being re-tasked by remote control to provide CCTV coverage of the area in question.

Another example is the case of intruder or fire alarm activation. These types of alarms may generate false positives - so called 'false alarms'. CCTV is often used to provide visual verification of the activation of these alarms and prevent nuisance calls to police and fire and rescue services.

Security systems are able to signal to operatives in centralised monitoring and control rooms with real-time alerts when RF (Radio Frequency) interference is detected. The presence of such interference, may indicate the use of jamming equipment, once again triggering a security response. Whether it is intruder detection wireless signals or Wi-Fi CCTV video information, security personnel are alerted to the potential of suspicious activity.

Systems that may be integrated with CCTV to provide layered protection include:

- Access control
    - Audio entry systems
    - Number keypad entry systems
    - Biometric fingerprint readers entry systems
    - Swipe cards/fobs ('token') entry systems
        - Includes 'binary' systems where two complementary fobs need to be presented, such as mother & baby tags for maternity units
- Alarm systems
    - Intruder alarm systems
    - Fire alarm systems
- Sound monitoring
- PA systems to warn trespassers off before committing intrusion offences
- Gates and barriers
- ANPR (Automatic Number Plate Recognition) vehicle identification

Layered cyber security

The central organising idea behind cyber security is the objective of protecting information.

Preventing unauthorised access to systems and data defends against tampering with the control of CCTV cameras and the theft and misuse of video data.

In the main, this means locking the network down to prevent access by hackers over the Internet. Best practice for information security architecture is to implement layered security by deploying a number of systems such as:

- Firewalls
- Security appliances
- Anti-virus software
- Heuristic email scanning services

To ensure an integrated system is secure, best practice should flow from ISO 27001, the quality standard for information security management.

Insider threats

Another important aspect is to defend against insider threats. Even networks that have been highly secured against external hacking may be vulnerable to data theft or misuse by people inside the organisation. Poor internal security controls may allow unauthorised as well as authorised staff to access the data.

For all organisations operating CCTV, the responsibilities of data protection compliance, including disclosure, sharing with police and preventing misuse by those inside the business, fall under the remit of the data controller.

Conclusion

For some, there is always going to be an interest in avoiding detection by CCTV; it is impossible to prevent criminals from developing new ways to disable cameras and the spread of such knowledge.

In the face of such a threat, the principle of layered security reduces risk. Multi-camera systems with real-time monitoring, alerting and analytics capabilities, integrated with other appropriate elements, and properly secured against cyberattack and insider threats, remain effective.

For the two audiences that may wish to understand how to avoid detection by CCTV:

Owners, operators, buyers, and commissioners

Integrated with other appropriate systems and operated correctly, CCTV remains an indispensable element in protecting people, property and premises.

Burglars and criminals

It's not worth taking the risk because a well-designed security system is going to detect any attempt at intrusion, so best not to bother...

SUMMARY

How iC2 helps you secure access to your CCTV system

iC2 is a leading mid-market security systems provider and was established in 2001. The business is owned and managed by a team with a collective experience of over 100 years in the electronic security business. iC2 holds CCTV and security accreditations with NSI and BSI.

Whatever methods may be devised to avoid detection by CCTV, iC2 works with the security industry to keep up with any developments. We install, configure and maintain all integrated security systems in line with or exceeding manufacturers recommendations, regulatory codes and health and safety requirements or guidelines.

Our security consultants design integrated systems to mitigate the risk of cameras being disabled. This uses the principle of layered security to trigger security responses in cases of alarm activation verification, or the detection of suspicious activity.

A prestigious client list including luxury international boutique brands, top flight sporting venues, retail developments and educational and social environments demonstrates how solutions are deployed to meet a variety of requirements.

From deterring theft of high value luxury goods, to sports fan and public safety and child protection, solutions are deployed to meet a range of legitimate purposes for which they are appropriate and fit for purpose.

REFERENCES AND FURTHER READING

In the picture: A data protection code of practice for surveillance cameras and personal information
ICO; CCTV Code of Practice; 2014
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

12 ways to protect CCTV from cyber attack
iC2CCTV
http://www.ic2cctv.com/white-papers/12-ways-protect-cctv-cyber-attack/

iC2 DESIGN INSTALL PROTECT

T: 020 3747 1800

E: info@ic2cctv.com

W: www.ic2cctv.com

About Us

Keeping you safe and secure at all times

iC2 provide you with innovative solutions tailored to you and your sector. We are London-based with a national team of surveyors and engineers that work closely with our clients throughout the UK and internationally.

Our unique consultative approach allows us to tailor bespoke systems to your individual requirements, ensuring that your operational requirements are met.

We appreciate the need to demonstrate the best value to you every time and as a technology-led company, you can expect our cutting-edge and ground-breaking approach to serve your needs for many years to come.

Please feel free to contact us to discuss any requirements you may have. We are happy to give you impartial advice, should you have any queries.