- Editors' Note……….……………......1
- Home Working Network Attacks Lead 2020 Scam Surge………………………..…...2
- How to Protect Your Kids Online with Parental Controls………………………………..….3
- How to Spot and stop Phone Tracking Apps…..5
- How to secure cannabis facilities with electronic door control and locking solutions…………..7

Issue 1 Volume 7 March 2021

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Security Solutions

Editor's Note

The year 2021 continued with a global pandemic, CoVid-2019. No one was prepared for this crisis which was first isolated in China and which now has covered the globe. This disease created new concerns that have created new approaches in security and how we as individuals deal with it. With countries launching and continuing with their lockdowns persons are forced to do everything from home.

The first article speaks about scams through your home network. A rise of 40% in the number of insecure links between work-from-home computer users and their work networks was detected since lockdown began.

The second article asks relevant questions how to protect your kids online. It discusses smart ways to keep the little ones safe in a time of online school and class sessions. In keeping with the theme of safety, the third articles examine how to spot and stop phone tracking apps. While these apps as useful for tracking your spouse and kids, it's a dangerous weapon in the arms of the criminals.

Article four discusses cannabis and it security while security is the core priority, a door interlock system deployed at cannabis facilities must also be user friendly and safe. This and other security methods are explored

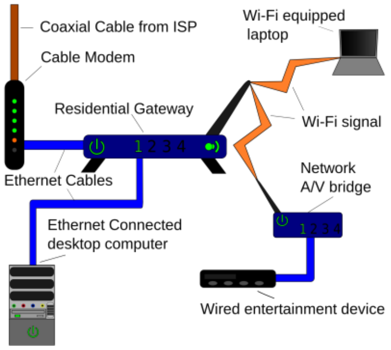
We do hope you find these articles and the safety methods helpful in some manner. We at **Amalgamated Security Services Limited** will hold steadfast and continue to fulfill our commitment, which is to provide quality service for all customers.

Regards
ASSL Marketing Team

Home Working Network Attacks Lead 2020 Scam Surge

The past few months of this crazy year have seen a huge scam surge and changing the most common types of con tricks.

Ninety percent of all websites relating to current health alerts are fakes, while stolen details of an estimated half million web conferencing addresses are being offered for sale on the dark web. That's according to Internet intelligence expert David Gewirtz in a mid-September update.



He's been researching how scam trends have changed in recent months and some of the most alarming traits. Here are some of the items from his list along with our tips on what to do:

* A rise of 40% in the number of insecure links between work-from-home computer users and their work networks. Separately, security firm Malwarebytes just reported that 1 in 5 of all firms say they've had a data breach directly as a result of home working.

What to do: If you're working from home, use up to date security and network software and check with your work systems people on what else you need to do.

* Connected with the above, a four-fold rise in just two months in brute force attacks enabling scammers to "guess" passwords by trying as many as they can.

What to do: Use apps, software and individual site settings that allow you to limit the number of password tries before locking a user out. Also, use two-factor authentication where possible, which requires a further security code or other ID. See https://scambusters.org/passwordsecurity2.html for more on this.

* A near 700% rise in just one month (March) in email scams relating to current outbreak topics. Malwarebytes also reports an increase of more than 1,200% in this type of message from January to April this year.

What to do: All emails from people you don't know should be suspect. Avoid clicking links, even in messages from people you do know. Consider messages telling you about cures and treatment as spam or worse. Use official health sites to monitor latest developments.

* More than 530,000 accounts using the web-conferencing program Zoom have been compromised. They're being offered for sale on the dark web at a penny a pop!

What to do: Zoom is the most popular work-from-home conferencing software. The firm has previously been criticized about its security, which has improved recently. Follow the firm's security guidance (https://tinyurl.com/Zoom-sec) and the advice in our earlier issue: https://scambusters.org/zoombomb.html

* Name adding. Software firm Webroot says it has seen a twenty-fold rise in phony and suspicious files using the Zoom name. It's being added to all types of attachments to try to trick people into opening them.

What to do: If you're interested in or want to know more about Zoom, visit www.zoom.us. Treat all Zoom conference invitations with suspicion until you've confirmed them.

By the way, our own research shows that individuals are being targeted by crooks who add the word "farm" to their identity and them apply for grants or loans available to the agriculture industry from the US Small Business Administration (SBA).

What to do: The SBA has its own security procedures, but you should also regularly monitor your record with the Big Three credit reporting agencies for any indication that someone has taken out a farm loan in your name. Tell them, the SBA, or any bank that is named next to the suspicious activity, then freeze your credit record. For more. See https://www.identitytheft.gov/

* Ransomware incidents, which lock up all the data on a computer or entire system until the ransom is paid (and sometimes not even then), have more than doubled so far this year.

What to do: Back up your system and data frequently and ensure your security software monitors for ransom attacks.

We can add to that list with:

* A big increase in pet scams as more and more people, isolated at home, opt to buy a cat or dog for some additional company. Most of these scams show up in online ads.

What to do: Adopt from your local animal shelter or buy only from breeders with a reputation you can check on and confirm.

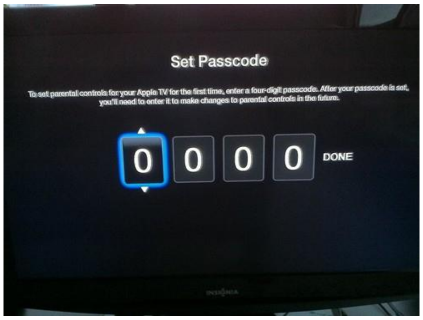
* Scams targeting visitors to 'adult' sites. In the current stay-at-home climate, these sites are seeing a huge increase in visitors. Certain sites harvest details about visits that may be passed on or sold. In other cases, crooks posing as online security officials, such as "Apple's Special Investigation Unit" call to say unpleasant or illegal photos have been found in your iCloud account. They demand payment to resolve the issue.

What to do: Just don't visit these sites. Then if you get an "official" call, you know you can safely ignore it. Plus, firms like Apple and Microsoft don't make these types of calls.

Interestingly, one positive aspect of recent events is that the number of unsolicited sales calls has dropped, probably because of the shutdown of call centers and furloughing of employees. However, if and when our health picture starts to improve, we expect to see a resumption of these and of mostly-illegal robocalls.

Reprinted from Scambusters.org

How to Protect Your Kids Online with Parental Controls


Set Passcode

To set parental controls for your Apple TV for the first time, enter a four-digit passcode. After your passcode is set, you'll need to enter it to make changes to parental controls in the future.

0 0 0 0

Your kids may already feel like you restrict and spy on their activities too much. But controlling their access to certain sites is an essential element of protecting them from scams -- and, possibly, protecting you from losing a lot money. Still, many parents are not sure of how to go about implementing these controls, just when many younger children may be about to fly solo online with their new Christmas tech gifts.

And as grown up as they may feel, restricting older kids and teens, or at the very least, sitting down and discussing the risks with them, should always be on the agenda.

Why You May Need Parental Controls

Kids and teens are one of the main markets for games and recreational software. And these days, they are also among the main users of educational programs. Like the rest of us, they're at risk of being scammed, lured into spending your money, compromised in some way or even cyberbullied. Using parental controls enables you to protect their vulnerability and, hopefully, your wallet. But controls can go way beyond that, for example by providing location tracking or ensuring data is properly backed up.

But before starting on implementation, you need to give some thought to the activities you might want to restrict. For example: amount of time spent on devices, the types of sites they can visit, their use of social media, and their ability to make purchases.

These are flexible restrictions and should be set up taking into account the youngster's age, experience, and trustworthiness! As they get older and more experienced, your parental controls naturally may change with time.

Implementing Parental Controls

There are five main ways you can limit or monitor your kids' computer access and online activities:

1. First, as we mentioned, discussing risks and agreeing on both restrictions and your monitoring access. If this works, it's probably the most effective parental control there is -- but that's a big "If"!

2. Then, the two main operating systems found on most home computers -- Microsoft Windows and Apple's macOS -- both come with built-in settings for parental controls.
The same goes for Apple's and Android's various mobile devices.

These enable you to do things like restrict access in terms of both devices and time, block websites, and manage spending permissions.

They're easy to get to and activate, both on PCs and Macs.

Microsoft has its own downloadable parental controls guide (https://tinyurl.com/Scambusters-2012031) but we found this page from How-to-Geek to be clearer: https://tinyurl.com/Scambusters-2012032

For the Mac operating system, visit: https://tinyurl.com/Scambusters-2012033. But again, check out this guide from iMore: https://tinyurl.com/Scambusters-2012034

For mobile devices, simply go to settings/screentime (iOS and iPadOS) or on Androids, visit the Play Store and click on settings/parental controls. For games devices like Xbox, you'll likely have to access settings through your account on a computer.

3. Controls built into apps and other software. These can often be found in the settings for individual apps, but in some games, including certain popular ones, they can be either difficult to find or non-existent.

The simple route is to launch an online search with the name of the app followed by "parental controls." We recommend you also do this if you're researching possible apps to buy as a gift or with a gift certificate.

4. Controls on specific websites. This mainly refers to social media sites like Facebook, Twitter, Instagram, and so on. But there are so many these days, and the site operators vary in the amount of help they provide.

Generally, you will have to visit the site's privacy settings on your youngster's device and work from there.

For the four of the most popular social media apps, here are some useful shortcut links:

Facebook:
https://tinyurl.com/Scambusters-2012035
Instagram:
https://tinyurl.com/Scambusters-2012036
Twitter:
https://tinyurl.com/Scambusters-2012037
Snapchat:
https://tinyurl.com/Scambusters-2012039

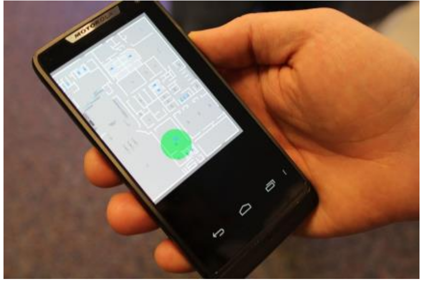
5. Dedicated apps -- programs that specialize in monitoring or controlling a device's activity. These include apps like NetNanny, Norton Family, and Bark (provider of some of the information in the links above). For a fuller list of the top-rated parental control apps, see: https://tinyurl.com/Scambusters-2012038

We started this list talking about the importance of discussing Internet scams and other privacy risks with your children. This is extremely important because, kids being kids, they may try to circumvent or unset controls. If they more fully understand why you are activating controls, they're less likely to do that. Plus, they'll be better armed as they head into adulthood, supported by your safety advice.

The question of parental controls is so important; we urge you to pass a copy of this issue to friends and families with youngsters.
Reprinted from Scambusters.org

How to Spot and Stop Phone Tracking Apps

How much do you trust your cell phone? Is it respecting your privacy or running a phone tracking app that lets others know where you are and what you're doing? And your phone knows an awful lot about you.



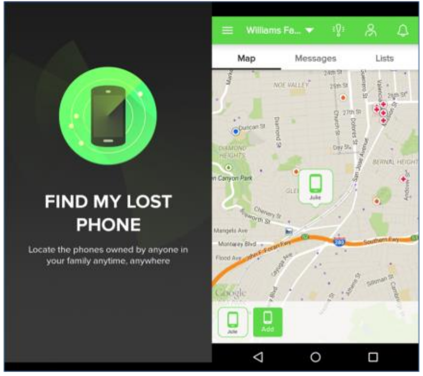
Phone tracking software is legally available for both Android and iOS (Apple) devices in the companies' official stores. It can have a legitimate purpose. For instance, it can be used by parents to keep track of their youngsters. But the same software also has less savory uses, such as spying on a partner or an employee. In some instances, it does more than just track the device; for instance, it might record phone conversations. And beyond this simple monitoring software, there's also off-store malware capable of stealing just about everything on your phone, if you let it.

As well as all these dubious activities, countless apps are legitimately capable of gathering location and even personal data -- with your permission (which they told you about in those Terms & Conditions you didn't read!). But don't panic. There's a lot you can do to spot and remove location spyware and to limit the extent to which your movements can be tracked.

Even so, it has to be admitted that the only way to guarantee your phone isn't being tracked is to switch it off -- as in powering down completely. And the only way to be 100% certain you don't have spyware is to return your device to its factory settings. Fortunately, you don't need to take such drastic actions to avoid most of the dangers.

Signs You May Have a Spy in your Phone. In most cases, spying on a phone's location requires someone to install the tracking software on the victim's phone. However, at least one tracker can work solely from a browser on the perpetrator's device. See: https://tinyurl.com/phone-track-tricks

That apart, it's not otherwise easy to install the phone tracker. The other person has to have access to the victim's phone -- either directly or via hacking and malware -- and know how to get around built-in security controls. The malicious app has to be concealed so the user doesn't spot it. But if you are one of the unfortunate ones to fall victim, or suspect you may be -- and more than one in a hundred phones are said to be compromised -- you can usually tell from increased activity on your device.


FIND MY LOST PHONE
Locate the phones owned by anyone in your family anytime, anywhere
Williams Fa...
Map
Messages
Lists
Add

You may also hear unusual background noise, like clicking and buzzing, although this is less common as tracking software has become more sophisticated. It may start to slow down or overheat, and the battery drains quickly. In some cases, it might keep rebooting itself or take ages to shut down. You might even spot an app, often with an innocent sounding name, that you don't recall installing. Or if your monthly data bill is inexplicably and sharply higher than normal, that's a powerful sign your phone is doing something you don't know about.

How to Remove Tracking Software

If you can't see the phone tracking app, you're probably not going to be able to uninstall it easily. But if you have security software on your phone, this might be able to identify it and remove it. Furthermore, some simpler tracking apps rely on your phone being continuously switched on, even when in standby mode. In this case, simply rebooting your device may actually flush out the tracker.

Some newer apps claim to be capable of detecting and removing trackers, but we haven't tested any of these so far. Otherwise, you either need to take your device to a tech expert or, as mentioned earlier, reset it to its factory state. Restoring your apps can take some time unless you have a backup that you made before the "invasion."

If you can actually identify the culprit app, you often can find specific uninstallation instructions online.

How to Avoid or Control Phone Tracking

The five most obvious ways or protecting yourself from phone trackers are:

1. Protect your phone. That is, keep it out of others' hands and be wary when using it on a public Wi-Fi network. Ensure access is password protected and keep your operating system up to date.
2. Install security software. You need to do this on both Android and iOS phones, although the latter are generally more secure. In addition to traditional security programs, you can install apps that warn you when a new program has been installed. And don't click on unfamiliar links, especially on social networks.
3. Don't "root" or "jailbreak" your phone. This tactic, which enables users to install unapproved or unofficial apps, is also one of the most common ways to circumvent device security.
4. When you install a new app, take the time to read through the Terms & Conditions so you know how much information the app is going to read, store, and even transmit.
5. Know how to limit the ability of legitimate apps to track you. Learn how to switch off tracking for each individual app and for your entire phone (though you likely can't totally eliminate it without affecting programs like mapping and weather apps).Of course, your phone service provider always knows which communications tower you're using, unless, as we said before, you actually switch the device off, which seems to defeat the whole purpose of having the thing in the first place!

Reprinted from Scambusters.org

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

How to secure cannabis facilities with electronic door control and locking solutions

Despite all the advanced security technology on the market, keeping product and cash locked down remains a basic rule

Bryan Sanderford

Cannabis business operations face a unique set of challenges that are both public-facing and anchored in strict government and banking compliance mandates. The one common denominator with these challenges is the need for tight physical security to better protect people, property, and assets with two predominant areas of interest focusing on entry/egress points, and back areas where cash is handled. Given all of the sophisticated security solutions available today, the most pervasive and effective physical security solution for cannabis businesses is to keep facilities, products and cash locked down. Door control technology continues to be a proven first line of defense to help prevent incidents from occurring, effectively keeping both customers and employees safe.

People usually think of doors as a means of keeping someone out, or alternately, keeping someone in. Doors provide privacy and, when locked, a level of security that is both simple and effective. Perhaps you never thought about it at length, but there are many ways that doors can be opened and/or closed. They can be manually operated with a handle or push bar, revolve, swing or even slid into a pocket in the wall – and they can be operated automatically with the push of a button, the swipe of a card or a proximity device, or be programmed to lock if another door is open or unsecure. All of these solutions are appropriate for specific applications in today’s cannabis facilities.

Controlling Physical Access

Perhaps the most essential aspect of cannabis business operations is also the most precarious – customer interaction and access to retail areas. This earmarks entry/egress control as a primary priority when implementing physical security measures. Fortunately, there is more door technology on the market today than ever before, including advanced programmable door interlock systems (often called mantraps), which provide very high levels of security. Door interlock systems provide cannabis facilities with a unique form of protection for both customers and employees that is not afforded by conventional access control systems.

Interlock systems have different names based on their functionality, and are commonly referred to as one of the following:

- Interlocks
- Mantraps
- Sally Ports (for vehicles)
- Secured Vestibules
- Air Locks

In its simplest form, a door interlock system commonly referred to as a “mantrap” is composed of two doors electronically connected so one cannot open until the other has closed. For cannabis facilities, an interlock door system can provide unrestricted access to an interior vestibule, where customers and/or employees can be screened automatically or by a security guard before entering your facility. Access to the interior of your operation is only allowed when the exterior door is closed, preventing tailgating of unauthorized individuals.

For retail locations, a secure vestibule may be employed. When an individual(s) in the interlocked area is approved, the outer door remains locked, and the individuals are allowed to proceed through the inner door. Conversely, if an individual is deemed suspicious, an alert can be sounded. The inner door will remain locked and the outer door will unlock allowing the potential threat to exit the building. This effectively prevents potential problems from escalating inside your facility.

For employee entrances, a secure-entry vestibule configuration provides a fast method of entry and egress through a combination of locked and unlocked doors. Exterior doors are normally secured and interior doors are normally unlocked. An electronic access system controls entry from the outside and a Request-to-exit (REX) device is used on the interior of exit doors. Unlocking the entry door will lock the interior door of the Secure Entry Vestibule. Once the exterior door is re-secured, the interior door is unlocked to allow access to the facility.

The highest level of security is provided with a restricted entry and exit system, whereby a door is unlocked by a request for access only if no other related doors are unsecured. Opening any one door keeps all other related doors locked. Restricted entry and exit systems will buffer simultaneous requests for access to prevent two or more doors from being unlocked at the same time. This door interlock system configuration is most appropriate for back areas of cannabis facilities where inventory is stored and cash areas are located.

For cannabis distribution facilities, sally ports can be deployed to control vehicular entry/egress using any combination of overhead doors, gates or bollards.

Door interlocks are also available with different modes of functionality. Cannabis facilities with a high amount of pedestrian traffic in the morning and late afternoon may want two doors operating during these time periods with the ability to switch to a single door during midday or evening hours. Intercom systems can also be added to door interlock systems to allow communications between the individuals inside the “mantrap” and a facility greeter or security guard controlling the system.

For employee access to highly secure areas within cannabis facilities, advanced interlock systems can be deployed with biometrics that read faces, eyes, and/or fingerprints to provide highly accurate identity authentication and verification, adding a much higher level of sophistication and security. This prevents lost, stolen, or replicated physical access control credentials or even simple key locks to be compromised by unauthorized personnel.

While security is the core priority, a door interlock system deployed at cannabis facilities must also be user friendly and safe, or it can become a logjam for customer traffic as well as a potential source of liability. In an emergency, the door interlock system must enable people to evacuate the facility. For example, if the power fails, an emergency override would ensure that the door can be opened manually. Moreover, safety codes may require that the door interlock systems be integrated with the facility’s fire alarm control panel to allow emergency door release. A local emergency pull station may also be required to allow doors to be unlocked in non-fire alarm emergencies or to interface the system with NFPA 101 delayed egress controls. In every case, local compliance mandates must be carefully adhered to when designing a door interlock system for your facility. Working with a reputable manufacturer and system installer ensures you will get the ease of operation and specific door interlock capabilities and compliance you need, along with high-quality customer support and service.

Door control solutions like interlock systems are highly cost-effective while delivering an effective means of securing your facility. Dortronics is a leading supplier of door control solutions and electronic locking solutions ideal for cannabis facilities. Our experienced team of door control experts are here to help assist with your specific needs with personalized support and products that are made in the U.S.A. We look forward to hearing from you.

About the author: Bryan Sanderford is the National Sales Manager at Dortronics. Please visit www.Dortronics.com for more information.

Reprinted from Securityinfowatch.com