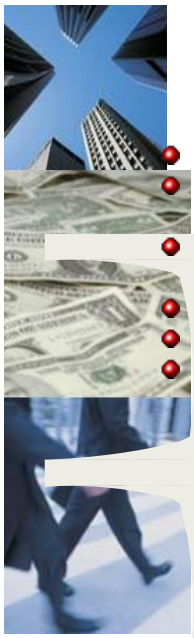

Issue 3 | Volume 9 | Sept. 2023

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Security Solutions

Editor's Note

Within the business setting, business owners along with their employees should make themselves aware of the scams and fraudulent acts that persons with bad intentions may do in order to gain an upper hand on your company by weaseling their way into your company software and hardware. With this harsh reality in mind we must protect ourselves from these acts by remaining vigilant at all times, never be lenient, never procrastinate, never take the easy way out when it comes to protecting yourself, your company and your assets.

The 2023 September edition of the Amalgamated Security Services newsletter explores the various ways persons may try to create havoc in your life and the lives of others within your organization. This issue focuses on crypto-currency, electronic surveillance, software protection and workplace violence.

Article one discusses crypto-currency or digital currency which is simply a way of transferring value from one person or organization to another, in a similar way to dollar bills. And like dollar bills, most cyber-currencies are only worth what people believe they're worth. Article two speaks to the professional dealing with illegal electronic surveillance. The issue of interception and eavesdropping protection is complex as both activities are developing very dynamically. Unfortunately there is no way to point out all aspects in one article.

Are you at risk of being tab nabbed? It's a sneaky trick hackers and scammers are using to access and change tabbed pages that you have open but not active in your Internet browser. Article three outlines how this is done and how to avoid being caught in this web trick. Article four focuses on registered lock codes particularly those assigned and registered to a user or company. These types of codes are usually used on high security locks as an effort to control access. The final article discusses why protecting against insider threats also protects against workplace violence

Knowledge of the aforementioned systems and scams, along with the knowhow on how to protect oneself and keep danger at bay is an important life skill within the workplace and in one's personal life. We do hope that you find these articles worth your time and the information is put to good use.

Regards
ASSL Marketing Team

Crypto - Currency Scammers Trade on Investor Ignorance

If you're an investor with an eye for novel money-making opportunities, you may have considered buying into a cryptocurrency. Plenty of people may have heard of cryptocurrencies -- Bitcoin is the best known -- but not a lot know what they are or how they work.

Which, of course, is one of the reasons why some investors want to get into them -- before everyone else does.

We don't have space to explain everything you need to know about them but here are the basics.

What is a Cryptocurrency?

A cryptocurrency, cybercurrency, or digital currency (they all mean more or less the same) is simply a way of transferring value from one person or organization to another, in a similar way to dollar bills. And like dollar bills, most cyber-currencies are only worth what people believe they're worth.

In the old days, dollar bills used to be backed by gold held by the U.S. Federal Reserve but that's not the case any longer. So, in one sense the bill is only worth the cost of the paper it's printed on. But because everyone accepts that it represents a dollar's worth of value, we can use them to exchange for things we want or need.

Many cryptocurrencies work in a similar way, except that they're numbers in a ledger rather than paper notes. They're worth whatever people are prepared to exchange them for. A few are backed by other things of value, like computing time or commodities, but let's not get too complicated here.

However, the important difference between dollars and digital currencies is that dollars are subject to control by governments and banking authorities. Cryptocurrencies have built-in security, but they are not controlled by any central authority, leaving them open to potential manipulation and abuse by scammers.

People buy and sell cryptocurrencies in a number of ways, but the main methods are through cybercurrency exchanges, market-traded funds similar to mutual funds, and through new issues known as initial coin offerings (ICOs).

Its ICOs we want to focus on because they're far and away the biggest sources of scams, which already run into hundreds of millions of dollars globally.

ICO Scams

There are already thousands of cryptocurrencies, each differing from the others in some way. Prices are usually very volatile, with investors trying to judge timing so they get in when prices are at their lowest and out at the top.

This makes new ICOs attractive to speculators and experienced investors. However, they've also drawn in inexperienced investors who hoped to make a quick killing but, instead, have lost millions either by misjudging the market or through ICO scams.

The basic scam process is fairly simple. An individual or organization announces the launch of a new cryptocurrency. They back it up with various types of documentation explaining how it will work and promising big returns. Investors pour into the ICO, and then the perpetrators disappear with the cash.
In other, more sophisticated, frauds, the founders of a new cryptocurrency fail to tell the

full story about their plans and their own ownership of the new "coin" or token. They actually keep a lot of it for themselves (never having actually bought it) and then sell as soon as they can.

Other variations follow the model of a Ponzi scheme in which some investors receive a return on their investment paid from new money that comes in from later investors who get their fingers burnt.

A recent article on Wired magazine's website noted: "The cryptocurrency market is ripe for scammers because it's relatively new, backed by tons of hype, and involves complicated technology. "It's easier to dupe someone into investing in your ICO in 2018 than your fake real estate business -- and plenty of people have.

"A cryptocurrency startup only needs a swanky website and an official-looking white paper. There are also plenty of services to help streamline the process: You can automate your ... sale or have someone write fake news articles hyping up your venture."

How to Avoid an ICO Scam

Often, the best way of spotting an ICO scam lies in what the launchers don't say rather than what they do.

If the issuer doesn't produce a synopsis, the White Paper referred to above, you can forget it. If they do issue one, this should outline long-term plans with a timetable, identify the names of the people behind it (which you can then check out), and provide proof of an impending listing on official ICO registries.

As with other scams, you should also be on the lookout for get-rich-quick promises (a real no-no).

Having said all of this, your best approach to ICO investment is to seek the advice of a qualified financial professional. When we say "qualified," we mean someone who knows and understands the cryptocurrency market.

No doubt, as the cryptocurrency world booms in the coming years, there will be genuine opportunities to achieve a good return on your investment. But there will also be an equally big chance of getting ripped off in a cryptocurrency scam. Take care!

Reprinted from Scambusters.org

If you are interested visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Professional Dealing With Illegal Electronic Surveillance

By Tomas Zilinskas

Not so long ago surveillance had been considered a government or spy agency priority. However a lot has changed. The rapid research and development in information technologies and electronic devices, along with their shrinkage in size has made surveillance obtainable by each of us. All you have to do is Google for GSM tracker, spy camera, hidden voice recorder. Don't be surprised to see hundreds of thousands or even millions of espionage gear offers. And it only depends on the commitment and financial constraints for one to start secret surveillance.

Thanks to the Chinese manufacturers tiny cameras, microphones and other tracking devices have become easily obtainable at a ridiculous price. The statistics of such equipment sales shows that many people are taking advantage of this hassle free access to modern eavesdropping technologies. The temptation to spy on the surrounding comes not only to perverted maniacs.

This article focuses on surveillance carried in interest

of businesses, politicians and simple ordinary (or not so ordinary) people.

The threat of eavesdropping & information loss has never been greater. Nowadays most exposed to eavesdropping are famous people, individuals with access to highly confidential information, companies and individuals as objects of corporate espionage, offices and individuals involved in political campaigns, investment bankers and other investment companies.

Here's the list of those who intercept most:

- Competitors or partners
- Employers against their employees
- Subordinates against their colleagues and superiors
- Tenderers against other bidders or against the clients
- Spouses and lovers
- Intrusives, maniacs
- Neighbors

The most commonly used espionage tools and methods are:

- Micro video cameras and recorders, often disguised as various household items such as watches, key chains, lighters, etc.
- Wireless and wired microphones of various types (radio, Wi-Fi, GSM, Bluetooth, laser, infrared, stethoscope, parabolic or shotgun microphones, etc);
- Eavesdropping software monitoring GSM phones, computers, laptops and tablets.
- Microphones transmitting information through the electrical grid, internet cables or security systems wiring.
- Devices intercepting the electromagnetic radiation of the computers, phones and other equipment for data processing and communication.

All the listed methods and devices can be considered just an illustration, as the actual number of devices can hardly be enumerated.

What's common for the above listed methods and devices that they are widely available, quite cheap to buy and their operation does not require any special technical skills. The equipment by having the access to internet either through Wi-Fi, cellular or stationary networks could be operated in any part of the World.

Detecting the bugging devices is not an easy and simple task. The term describing this type of activity is TSCM which is the abbreviation of Technical Surveillance Counter Measures. TSCM survey is a service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility. A TSCM survey normally consists of a thorough visual, electronic and physical inspection inside and outside of the surveyed facility. In conducting surveillance protection one has to be familiar with the tapping methods; hardware and software products; engineering solutions used for this purpose as well as their unmasking signs. Without this knowledge it is not possible to detect a well hidden bug.

For the successful implementation of this activity it is necessary to have properly trained personnel, good working methodology and an appropriate set of technical means.

As there are lots of methods of eavesdropping and much more devices used for each method, there are lots of instruments to detect a bug. Examples of the necessary equipment for the detection of radio microphone is radio frequency spectrum analyzer, wideband radio receiver and a nonlinear junction detector (NLJD). And

this should be considered the absolute minimum.

The issue of interception and eavesdropping protection is complex. Both activities are developing very dynamically. Unfortunately there is no way to point out all aspects in one article. Practice shows that the systematic work and the funds invested for eavesdropping protection are sooner or later paid off.

Article
Source: http://EzineArticles.com/expert/Tomas_Zilinskas/2531015

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

Tabnab Scammers Hijack Web Browsers

Are you at risk of being tabnabbed?

It's a sneaky trick hackers and scammers are using to access and change tabbed pages that you have open but not active in your Internet browser.

Here's the deal:

When most of us use an Internet browser, be it Chrome, Firefox, Internet Explorer, Edge or Safari, we often open multiple pages and keep them open so we can move back and forth between pages. We do this by clicking on the tabs for each page, which are helpfully inserted by the browser.

Now, think back to what happens if you open a bank web page or some other site where you store confidential information, like sign-on details. Oftentimes, these secure sites will log you out if the page is inactive for a certain amount of time. Then, when you revisit it, the page tells you that you've been signed out and asks you to sign in again.

What a tabnabber does is take control of that page while it's inactive and replace it with a replica of the genuine page. Then, when you sign on again, you inadvertently give away your sign-on details and maybe other confidential information.

That's tabnabbing. It's a clever phishing trick and it’s been around for many years, exploiting the way web pages are scripted (written) to perform the trick.

In some cases, hackers may completely change an inactive page to one they know or suspect the user might visit from time to time -- for example, changing a Wikipedia page the user had open to, say, a fake but genuine-looking Citibank sign-on page.

Inattentive

They're hoping that the user will be sufficiently inattentive to think they must have previously opened the Citibank page, so they sign on, giving away access to their account.

The scam originally focused on spoofing the sign-on page of Google's Gmail service but now, according to security services, it can be used to fake just about any site. It also changes the "favicon" for the page -- the tiny icon that appears next to the page title in the tab.

And once the crook has your

sign-on details, they can visit your account wherever that might be (even if it's a non-financial site) and find other information about you that's useful for identity theft, such as the answers to security questions, home address, Social Security numbers and date of birth.

The trouble is -- and this is what makes tabnabbing particularly effective -- that we tend to trust our browsers and those handy tabs, switching from one to the other without thinking and often not taking the time to check on security. For example, how often do you bother to check the address line of a particular page to be sure it begins with the secure "https" label instead of the non-secure "http"?

3 Actions

There are three things you can do to eliminate the risk of being a tabnab victim.

First, get into the habit of closing tabs when you've finished with a particular website. If you have to reopen it, at least you'll be keying in the correct address from the outset.

Second, if you do leave your tabs open, be alert to which contents should be shown there. If the page is different to the one you thought it should be, close it.

Third, just to be doubly sure, if you revisit a tabbed page that says you've been signed out and invites you to sign in again, close the tab and start over.

Some browsers offer extensions (mini add-on programs) that claim to be able to stop tabnabbers, while others claim that by disabling JavaScript (a programming language used on certain web pages) you will be secure.

However, other security experts suggest these may not be totally effective and that hackers have found a way around these defenses.

Alternatively, if you use a password manager that automatically inserts your sign-on details, this will likely check to see if the page is the same one where you originally saved them. If not, it will simply not enter the information -- a clear red flag signaling trouble ahead.

Tabnabbing is not new. It's been with us for many years. But the fact that it is still around and in widespread use indicates how effective it is. Beware!

Reprinted from Scambusters.org

Synopsis to use for the email Tabs that allow you to keep multiple pages open in your web browser are the target for a sneaky phishing scam called tabnabbing. By secretly changing the content of inactive pages, hackers can trick you into giving away confidential information about yourself. In this issue, we explain how tabnabbing works and what you can do to beat the tricksters.

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

What Is A Registered Lock Code?

By George Uliano

Before we discuss a **Registered Lock Code**, lets discuss just what this is. When a lock is assembled pins are placed inside. These pins allow the opening and closing of the lock with the key. There must be a way to transfer the locking pins to cuts on the key. This is called the code.

A registered lock code is assigned and registered to a user or company. Only authorized users can order cut keys. These types of codes are usually used on high security locks as an effort to control access. Our Company will maintain these in a custom designed computer database. This database will help to avoid repeating the codes so once assigned they will never be duplicated or assigned to another user.

These types of codes are usually "Blind". This means that by looking at the number you will not be able to convert it to a key cut. A lock code chart is needed to convert the code to a key cut that will match the locking pins in the lock and operate it.

With many non-registered codes, it is very easy to convert the code to a cut. For many, the code is the cut. This lowers the overall security as it gives no key control. Key Control is the ability to know how many keys were cut for a code and who ordered those keys on what date. Key control and registered lock codes go together.

High security locks are usually found at authorized service centers, such as Locking Systems International. They are more expensive than big box store products, so you first must decide what you are protecting and how much is that worth to you. After making that decision, you will know where to make a purchase.

When you purchase a high security product, registered codes are assigned to you. By keeping these codes you will be able to order additional keys later. The number of registered codes you get depends on if you order locks keyed alike, keyed different or master keyed. For example, if you order 10 locks keyed alike you will get one registered lock code. If you order 10 locks keyed different you will receive 10 registered lock codes.

I hope this isn't too confusing. The biggest take away here is that high security locks and registered lock codes go together.

George Uliano is a security professional with years of law enforcement and security experience. He earned a Bachelor's Degree in Criminal Justice and Business graduating with honors. George holds three U.S. patents on different locking principles. This combination gives George and His Company Locking Systems International Inc the unique ability to provide its customers with the correct security at an affordable price.

For additional information or to purchase Locks go to http://www.lsidepot.com

Article Source: http://EzineArticles.com/expert/George_Uliano/1500014

If you are interested visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Why Protecting Against Insider Threats Also Protects Against Workplace Violence

By Diane Griffin

According to the Occupational Safety and Health Administration (OSHA), nearly 2 million employees are victims of workplace violence each year. An even more startling statistic is that between January 2009 and July 2015, there were 133 mass shootings in the workplace. No wonder violence in the workplace has become a top security concern for all employers

.

While there isn't a federal law preventing workplace violence, OSHA requires a company to provide employees a workplace "free from recognized hazards that are causing or are likely to cause death or serious physical harm." This is a lot easier said than done now that technology has expanded our work environments to places outside of our physical office buildings. I don't believe it is a coincidence that we are seeing an increase in workplace violence as well as insider threats-after all, when we fail to detect and control internal threats we are not only jeopardizing our brand but also the lives of those who work with us and for us.

As an employer, you could be held liable for negligent hiring or for failing to conduct a basic background check. You could also find yourself in hot water for not establishing or implementing a zero tolerance policy for those who use the workplace-and work issued tools such as computers and cellphones-for harming others. This would include threatening, stalking or harassing anyone at or outside of the workplace.

Preventing insider threats is one of the best ways to protect your employees and yourself from workplace violence. Here are just a few things you should be doing:

Don't Skimp on Background Checks

Be sure to have a standard screening policy that includes what checks should be performed for each position as well as what information you need to gather such as previous employment and criminal background checks. Always look for inconsistencies between information and documents and address the issue immediately. I also recommend expanding your background check policies to include a repeat screening-just because an employee has a clean record on the first day of their employment does mean the record will stay clean.

Monitor Online Actions of Employees

If you do not currently have a system in place for monitoring the online actions of employees, you need to create one. This type of system will allow you to discover suspicious actions before they become more serious. Monitor your employees online and always consult with your legal team.

Have an Employee Exit Plan

As soon as an employee has left the company, be sure to not only collect any technology he or she may have been using but immediately prohibit access to servers, networks, and content,

even if that means immediately disabling accounts.

Companies must prepare for workplace violence the same way they prepare for insider threats-by taking the steps needed to prevent these situations from occurring. A little planning can go a long way towards keeping your business safe.

Article Source:
http://EzineArticles.com/expert/Diane_Griffin/717287

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