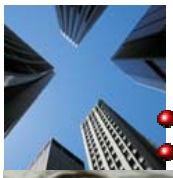


Issue 17 | Volume 1 | September 2015

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note

Within the business setting, many business owners along with their employees have to be 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 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 organisation. This issue focuses on email threats and software protection as these are increasing vulnerabilities for most persons.

Article one and two both deal with bogus emails that can jeopardize your security and that of your organisation. Here we learn how these emails target employees along with stealing the business identity. Scammers don't only steal your money or company assets, they now have new tricks where they steal and trade your airline miles. Article three outlines how this is done and how to avoid being caught.

Article four deals with ransom ware which is software that locks up your computer until you pay the "ransom" to scammers. Unfortunately this has arrived on smart phones. This shows how important it is to secure your software.

Securing your physical property for burglary and other hidden dangers is of highest priority and article five and six deals with the type of padlock selected and fire extinguishers respectively.

Knowledge of these and other scams, along with the knowhow on how to protect oneself and keep danger at bay is an important life skill. We do hope that these articles are worth your while and we do hope that the information is put to good use.

Regards
ASSL Marketing Team

Bogus Business Email Targets Employees, Costs Millions

What would you do, supposing you work in the accounts department of your employer, and you got a business email from your boss telling you to change the way you pay invoices?

Here's hoping you'd check the instruction with the boss or another key figure in the business. Otherwise, you could be playing an unwitting part in a scam that could cost the firm a fortune.

According to law enforcement officials, scammers who have hacked their way into company computer systems have been sending these redirection emails to employees in the finance section of small businesses. They tell the employees that, instead of sending checks to specified suppliers, they now have to send the cash by electronic transfer.

We all recognize by now that wiring money can be a dangerous payment method if you don't know the person you're sending it to. But in this case, the victims think they do know who they're sending it to, and with their guard down, fall for the scam.

According to the FBI, this scam, which they call the Business Email Compromise (BEC), cost one Tennessee company $850,000.

In another version, the scammers pose as a supplier to the company and simply ask for payment of invoices to be wired instead of being paid by check. The cash ends up overseas and cannot be recovered. The scam, the FBI reports, is global, with victims in 45 countries and all U.S. states, and costing firms a total of $215 million.

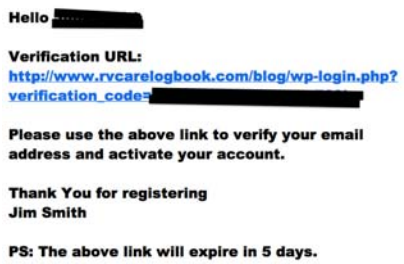
Action: If you're in a position to make payments for your company, be on the lookout for these scam emails and report them to manager.

It means not only that someone is trying to scam you but also that they most likely have hacked into your company systems and could put other elements of the business at risk. And if you happen to be a small business owner, be aware of and alert your employees to the danger. Perhaps even have a system where more than one person has to approve changes in payment processes.

Employee Phishing

Another sneaky way that hackers target employees is by sending emails that pretend to be from the company HR department or someone with an HR function in a business.

The message tells the victim the firm is changing his/her employment status and they have to click a link for more details. The message looks genuine -- so who wouldn't be desperate to click? But the link takes victims to a spoof site that looks like the firm's real site, where they're asked to log on with their company email address and password. It then provides some innocuous information that puts the employee's mind at rest.



Hello [redacted]

Verification URL:
http://www.rvcarelogbook.com/blog/wp-login.php?verification_code=[redacted]

Please use the above link to verify your email address and activate your account.

Thank You for registering
Jim Smith

PS: The above link will expire in 5 days.

Meanwhile, the scammers use this information to sign on to the victim's genuine company account and change bank details so that their wages are sent to the crooks' account.

Action: Be immediately suspicious if you get this email; don't click the link.

Most firms would be unlikely to notify you of changes this way, but you should either contact your HR people by phone or sign in to your account independently and check details from there.

Business Identity Theft - Three Keys to Protection

By Warren Franklin | Submitted On June 02, 2015

Imagine discovering you are the co-owner of your business instead of the sole owner, or that you have a satellite business you didn't know about operating in a different state, or there is a business with a similar name using a similar address to yours pretending to be your business. How would any one of these scenarios impact your business? This is what business identity theft looks like. It can happen to any business large or small. It could happen to yours, too.

Most small to mid-sized businesses don't understand what identity theft can do to their business until it is too late.

Business identity theft doesn't target individuals; instead, criminals look for ways they can take valuable information from legitimate businesses. They are looking for bank accounts, credit card numbers and passwords, and sensitive intellectual information.

These looters gain access to key accounts and drain them, many times, before the bank is aware of the act. The cost of business identity theft can be enormous. It could take hundreds of hours and a large sum of money to repair the damage. Some businesses never recover and go out of business.

Business identity theft is still a relatively new type of crime. Most business owners haven't heard of it. So there is a temptation to ignore it. Steve Cox of the Better Business Bureau says, "Business identity theft is a very real concern in today's marketplace. From a criminal's perspective, it's significantly more cost-effective to steal business identities than consumer identities.

The criminals act quickly. They know they only have a short period of time before the act is discovered. The Ponemon Institute says that in 84 percent of the cases money was stolen before the fraud was detected by the bank.

Many small business owners don't think they have much that a thief can take from them. But the truth is that you don't have to have more than a good name. The thieves can use it to get loans, order products and ruin the businesses good name. Dun and Bradstreet's Senior Risk Analyst Robert Strezze states, "What is particularly disturbing about this trend is the significant dollar amount involved. It's not unusual for the losses to be in the mid-six figures by the time the criminal activity has been detected."

The unfortunate truth is that most businesses don't take the time or steps to safeguard against the crime. Most are too busy doing the daily activities to keep the business going. It isn't until the damage is done that a business realizes the trap it fell into.

What are the keys to business identity theft prevention?

There's good news for businesses who are willing to put some time and effort into business identity theft prevention. Many times preventative measures can mean big savings and a better image in the community. There are three keys where a business can lessen the likelihood that identity theft will happen:

The first key is to establish a position on the leadership team that is in charge of monitoring for business identity theft, establishing procedures for data breach prevention, and protect against other criminal activity. This officer could be called the Chief Security Officer, for

example, and should have the power to check banking, credit card and other key accounts. The officer would be wise to establish "best practices" for information security including employee training, password protection and more.

The second key is to set up monitoring services that watch your back for you. A business's personal information is everywhere. It is nearly impossible for one person to keep an eye on every aspect of the business. A business identity theft protection service that includes business credit monitoring and internet surveillance, identity theft alerts, and whole business recovery can be a valuable asset for identity theft protection.

The third key is to set up credentials monitoring in the Dark Web. This is where criminals do their business buying-selling-trading stolen information. Credentials monitoring will alert a business when stolen credentials, IP addresses and, for banks, BIN card numbers appear. Businesses can take proactive steps to prevent the stolen information from harming them, their employees and/or customers. Millions of stolen credentials, email and login information, show up every month. Stolen credentials is a major player in all forms of business fraud.

Business identity thieves are clever and determined. They can take advantage of businesses and business owners that do not take precautions to protect their business.

I ask nearly every business this question: "If someone started representing himself as an owner or officer in your business, how would you know? How soon would you want to know?

How many times have you discovered an error after it happened? For most of us, it happens all of the time. Generally, we can get past it without much harm. However, an error of not protecting your businesses' identity is something that you won't get over easily. You can learn more about identity theft protection by going to http://franklinrms.com/idefendbusiness.html. I recommend monitoring credentials and IP addresses to make sure you catch criminal activity before it negatively impacts your business. You can learn more at http://franklinrms.com/cyberid-sleuth.html. Education is a must when it comes to protecting a business. This is your chance to learn about the problem and the solution. I have been involved in the information security field for over 10 years. I have trained hundreds of individuals in this field and been a speaker at many events. You are welcome to email me at warren@franklinrms.com. I welcome your comments and questions.

Article Source: http://EzineArticles.com/?expert=Warren_Franklin

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 Scammers Steal and Trade Your Airline Miles

The theft of millions of airline miles from accounts at two big U.S. airlines provides proof, if it were needed, that you should never use the same password on more than one valuable online account. As many as 10,000 accounts at American and United Airlines were accessed by crooks -- but not by directly hacking them. They apparently got the usernames and passwords by hacking third party servers not connected with the airlines.

Then they used these to try to sign on to the airline accounts. Where they succeeded, they stole the points, using them to buy gifts and book or upgrade flights. If users had different passwords, this could never have happened.

The incident happened several months ago and the airlines say they will be notifying customers whose accounts were affected. Even if you're not one of them, it's probably a good idea to change your password if you have a frequent flyer account with either airline and if you're using one that is duplicated for other accounts.

For more information about password security, check out this Scambusters issue:

http://www.scambusters.org/passwordsecurity.html

Fortunately, it seems that other confidential information attached to people's accounts, including their credit card details, were not compromised. However, the theft highlights the growing attractiveness of frequent flier miles to hackers, with one observer saying that points have become a sort of currency that is used and traded on black markets.

The fact that you can trade points for a wide range of products, not just travel, makes them extremely attractive.

Bogus Miles Awards

This isn't the only tactic scammers are using to try to steal frequent flier miles. In both the U.S. and Canada, they're using robocalls to tell individuals they've been awarded thousands of extra points. The calls claim to come from the Canadian company Air Miles, airlines Air Canada or WestJet, or online travel company Expedia.

The call invites recipients to press a key to proceed with the mileage points claim. This connects them with an operator who asks for airline account details or other confidential information that might be used for identity theft.

Action: This scam has been running for several years and is ongoing.

It's easy to tell if you're being targeted. None of the companies mentioned uses this type of robocall marketing -- it's illegal anyway in most cases.

So if you get a call, it's a scam.

Phony Sales of Miles

In yet another airline miles scam, crooks pose as brokers of unwanted miles, which they offer for sale via sites like Craigslist. Or sometimes, they claim to work for the airlines industry and have more free miles than they will ever need. By suggesting, for example, that they're senior crew, like pilots, they add an element of credibility to their con trick.

Often, victims are in a hurry to buy the miles, which makes them a perfect target, willing to either wire cash or use a prepaid debit card to pay for them. You send the money and that's the last you hear of the "seller."

Action: Buying airline miles this way is highly risky. So,

don't.

In the cases we researched, one victim received phone calls and even copies of a driver's license from the scammer. This supposed proof of identity turned out to be worthless.

One clue to the scam is that the crooks usually offer the miles at extremely low cost -- the first red flag.

But the key, as ever, is the request to wire cash or use prepaid debit cards, both of which are untraceable.

Airline Warnings

Several airlines have posted warnings about mileage / points scams. For example, American Airlines has a whole list of phishing emails at https://www.aa.com/i18n/urls/phishingEmails.jsp, together with a list of characteristics of bogus emails.

United offers a customer care inquiry form at https://www.united.com/web/en-US/content/Contact/customer/default.aspx?camp=virtual_expert

That's it for today -- we hope you enjoy your week!

Ransomware Holds Smartphones Hostage

It was probably inevitable, but ransomware -- software that locks up your computer until you pay the "ransom" to scammers -- has arrived on smartphones. The malware that seizes control is targeted mainly at Android phones. It flashes up a message claiming to be from the FBI, a government cyber task force or a security firm, claiming that the user has been accessing illegal websites and must now pay a fine to get access to their device again.

A typical message fills the full screen of the phone with text that includes "FBI Criminal Investigation - Prohibited Content." It continues, "This device is locked due to the violation of the federal laws of the United States of America," and goes on to list the supposed articles of law that have been infringed.
Because it's a crooked operation, payment, of course, must be made by an untraceable money wire or preloaded debit card, the number for which has to be provided to the scammers.

Ransomware has been around for years but mainly on Windows PCs, and we've reported on it several times.

http://www.scambusters.org/ransomware.html

http://www.scambusters.org/ransomware2.html

These types of PC ransomware attacks are still in full flow, according to a new report from hardware maker Intel and security firm McAfee. Meanwhile, a new "DIY" program that enables crooks to build their own ransomware is contributing to what the report labels a "meteoric rise" in this crime.

Cell Phones Bombarded

The attack on cell phones is relatively new, however, but it has already bombarded more than a million devices. According to a report from the New York Times, some 900,000 users were targeted in just one month with a piece of malware called "ScarePakage." Other variations of the malware have also been identified.

It's easy for the unwary to be infected, either via a malicious app disguised as legitimate or by visits to certain "adult" websites. The malicious programs are most commonly downloaded from app stores

other than Android's official Google Play store, though some have even found their way there.

Of course, it's not just ransomware that threatens the safe use of smartphones. There are also malicious programs that can steal information, record calls for blackmail and extortion, send out spam, and wreak havoc with usability. Leading security software company Norton recently warned against assuming that any app is safe. "There are now hundreds of thousands of apps available," Norton says. "Even if your source for an app is legitimate, it can be impossible for the official stores to police every app. Always use good judgment before downloading an app."

Actions you can take to cut the risk of getting infected include:

* Check an app's trustworthiness on the free www.mobilesecurity.com website.
* Avoid visits to dubious/questionable websites.
* Be wary about using non-Google app stores.
If you know how to do it, uncheck the setting that allows you to download apps from "Unknown Sources."

* Also be wary about downloading and installing brand new apps for which there are no user reviews, or apps that only have a few users.
* Use a passcode that will prevent anyone else from directly accessing your phone and downloading malware into it.
* Install security software that can detect malicious software. Again, this mainly relates to Android devices.

To find an app that suits your needs, simply do a search using the term "security" on Google Play.

Should You Pay a Ransom?

Should you pay a ransom demand? No, say the experts. Your best course of action is to keep regular backups of your device setup and reinstall this -- either yourself or with professional help if needed.
In some cases, you may be able to restart your phone in safe mode and delete the malware from there. If you're not expert enough to do this, again seek help from a trusted tech professional.

If you do pay the ransom -- usually around $250 -- there's no guarantee the crooks will give you the code to unlock your phone, assuming they even have one. And if they do have one that you successfully use, the scammers will almost certainly still have access to your phone from which they can continue to steal information.

What's next? We think wearable devices will be next to be targeted by the ransomware crooks. More on this another time.

Alert of the Week: Some good news for a change. As from late June, some banks have started using the suffix ".bank" (dot-bank) in their Internet addresses.

Since banks will be carefully vetted before they're allowed to use this suffix, the hope is that it will add another level of security to online banking -- in the same way that ".gov" (dot-gov) indicates a genuine government website (provided it's at the end of the main address). The switch will probably take many months to complete. Look out for the change from your bank.

That's all for today -- we'll see you next week.

Reprinted from Scambusters.org

Padlocks - Mechanical to Electronic

By George Uliano | Submitted On June 01, 2015

When you think padlocks you probably picture a rectangular piece of metal with a loop on top. Today there are so many types of padlocks that it would be impossible to discuss them all in this article. My purpose here is to give some understanding of the many types of padlocks and what they do. When you purchase a padlock the first thing that you must consider is what you are going to protect and how much is that worth to you.

Once you answer that question it's time to choose your padlock. Here are the major components:

Padlock Body: This can be made of many different materials from plastic to hardened steel. It can be as small as a luggage padlock up to, well, any size. The body can take any shape such as round or square. The two most popular types of padlocks are made out of brass or steel.

Let's look at these two:

- Brass bodies are best used near water or high moisture areas
- Brass bodies might be plated in nickel, which might make you think that it is steel
- Steel bodies are either hardened steel or the popular lamented plates
- Locking balls should be used for strength, these are located where the shackle goes into the body, when locked these steel balls engage the shackle to provide locking on either side

Shackle: The shackle comes in many different lengths and thicknesses. It can be made of different materials. The shackle is normally made of hardened steel. This is done to increase the cutting strength. Also, the larger the diameter of the shackle the harder it is to cut. When choosing a shackle, choose the shortest length to do the job. For example if you choose a two inch shackle where a one inch shackle would do the job, you are leaving one extra inch for someone to cut or attack.

Lock Cylinder: The lock cylinder can be anything from a single bitted mechanical lock all the way to the highest security electronic lock. You are probably thinking that you don't have a choice, you go into a big box store pick out a padlock and you get whatever lock cylinder it comes with. That is true with big box store padlocks. However by contacting a Padlock Service Center you can get a padlock custom made with whatever lock cylinder you need.

As I stated earlier the most important decision is what are you going to protect and how much is that worth to you.

George Uliano is a security professional with years of law enforcement and security experience. He earned a Bachelors 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

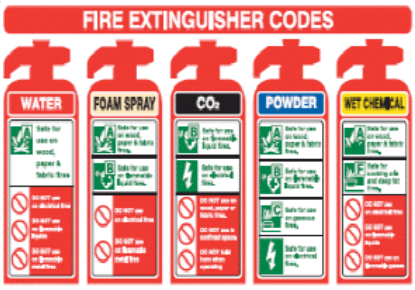
Article Source: http://EzineArticles.com/?expert=George_Uliano

If you are interested in learning more about our home security systems visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Fire Extinguishers - Which One to Use and How to Use It

By Liam Swann | Submitted On June 20, 2014

Almost every home and every company around the world will have at least one fire extinguisher. In most companies there will be more than one, possibly one in every office and room in the building.



You will notice that they are all the same, whether you have a small one in the kitchen at home or a large one on the wall at work, they are all red in color, but the difference is that they have different colored labels. This helps you differentiate between the different fire extinguishers and it's important you know which is which, because each one works on different materials.

There is no point grabbing the first one you see in the event of a fire and spraying the fire, only to be using a wet fire extinguisher on electrical cables. Get to know what each color code is for and what it works on, this can help you grab the right device in the event of a fire, possibly combating the flames and calming the hot spots before the fire department arrives.

The first one you will notice is the red canister with a red label. The red label is the water canister and this can be used on paper and textiles, never use on liquid or electrical fires.

The next one is the red canister with a blue label. The blue label is for powder, this is the one you want to grab in the event of a liquid or electrical fire. It also works on wood and paper, so this is probably the one you will see in the office.

The red canister with cream label is the foam option, which works well on wood fires, paper, textile and liquid fires, such as petroleum, for example. Never use the foam canister on electrical fires; you can cause considerable damage, not only to your offices but to the entire building.

The black canister is designed for use on liquid and electrical fires and these are often found in factories and industrial sites.

Finally is the yellow label, this is the wet canister which is used on wood, paper and cooking materials. This is the one that you will find in your kitchen at home or in a commercial kitchen, either in a restaurant, pub or hotel.

Now that you know how to differentiate the different fire extinguishers, you need to know how to use them. Your company should provide you with adequate fire safety training, which is a must for all staff at any business. In the event that your training didn't cover how to use these devices, they are simple to use, as long as they have been serviced and Firstly before you do anything, check the pressure on the canister. It should have good pressure, preferably full. Standing a good distance from the flames, you will want to pull out the pin, when you do this it breaks a seal, enabling you to use the fire extinguisher to fight the fire.

Don't be a hero, if the flames are getting too out of control, it's time to leave and let the fire department sort out the problem. In the event the fire has just started and the fire is moving horizontally along the office floor, you will want to gently squeeze the lever and aim for the base of the fire, moving across and back. Should the fire be reaching for the ceiling, then you want to gently squeeze the level while starting at the base and then moving upwards and back down again.

If you are successful and manage to put out the fire, concentrate on any hot spots to reduce the risk of them re-igniting, then evacuate the building and wait for the fire department with everyone else.

S K Fire Protection is an established UK fire safety and equipment specialist offering products and training throughout the United Kingdom. This company offers a host of fire safety services including fire extinguisher servicing, inspections and replacement, fire risk assessments, training and much more. With over sixty years' experience in the industry, S K Fire Protection ensure their customers receive the highest quality service by experienced and knowledgeable contractors. The company has a number of professionals operating from outlets throughout the country offering superior service to business and homeowners. To find out more about S K Fire Protection, visit their website at http://www.skfireprotection.co.uk.

Article Source: http://EzineArticles.com/?expert=Liam_Swann

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