ACT SMART I.T.
www.ACTSmartIT.com
General Business Edition – July 2024

Securing Your Business

As your technology evolves, so do your business' risks. Hackers have become more sophisticated and utilize the Dark Web to purchase ransomware schemes, access to server credentials, credit card accounts, and many other nefarious activities.
Here are some of the most important things you need to know:

1. You Aren't Too Small to Attract Hackers
Small Businesses Are Especially Vulnerable

Given that small businesses have fewer resources to dedicate to cybersecurity, it is unsurprising that they are more vulnerable to cyberattacks. In fact, 43% of all cyber attacks are directed at small businesses. If you're running a small business, it is critical to take data protection seriously and invest in robust cybersecurity measures that can keep your organization safe.

Enclosed you will find our Phishing Postcard to put near your computer as a reminder. If you would like complimentary copies for every computer in your office, go to ACTSmartIT.com/phishing. The first step in protecting your business is to identify the assets that are most important to your company. This includes financial data, customer information, or intellectual property. Your assets also include the hardware your company runs on. If the hardware is rendered inoperable from a cyberattack, the inability to transact business can be equally devastating.

2. Phishing Attacks Are a Major Threat

Cybercriminals have an endless arsenal of methods to infiltrate a company's systems. However, one of their favorite tactics is phishing. This involves sending an email that appears to be from a legitimate source but is meant to trick people into revealing sensitive information such as passwords or bank account details. In fact, as many as 90% of data breaches occur as a result of phishing attacks. If your organization wants to stay protected, it's crucial to be vigilant about phishing attempts and take steps to minimize the risk of falling victim.

If you'd like complimentary copies for every computer in your office, go to: ***ACTSmartIT.com/phishing***

3. You and your employees could easily be scammed!
Today, AI makes it even easier for a scammer to trick you into sending money, making changes to financial records, disclosing sensitive information or allowing access to critical data.

- **Scammers pretend to be someone you trust.** They impersonate a company or government agency you recognize to get you to pay. But it's a scam. Artificial intelligence can even impersonate a voice. If the request is unusual, hang up and call the person back using a number that you know, not the number on caller ID.
- **Scammers create a sense of urgency, intimidation, and fear.** They want you to act before you have a chance to check out their claims. Don't let anyone rush you to pay or to give sensitive business information.
- **Make sure procedures are clear for approving purchases and invoices, and ask your staff to check all invoices closely.** Pay attention to how someone asks you to pay and tell your staff to do the same. If someone demands that you pay with a wire transfer, cryptocurrency, or gift cards, don't pay. It's a scam. Since scammers often fake their phone numbers, don't trust caller ID. If you get an unexpected text message or email, don't click any links, open attachments, or download files. That's how scammers load malware onto your network or try to convince you to send money or share sensitive information.
- **Scammers sometimes even hack into the social media accounts of people you know,** sending messages that seem real — but aren't. Be wary of what you and your team post on social media. Too much information give scammers credible facts that can make them more believable.

Continued on Page 3

From The Desk of David Snell

WOW! Summer is HERE!

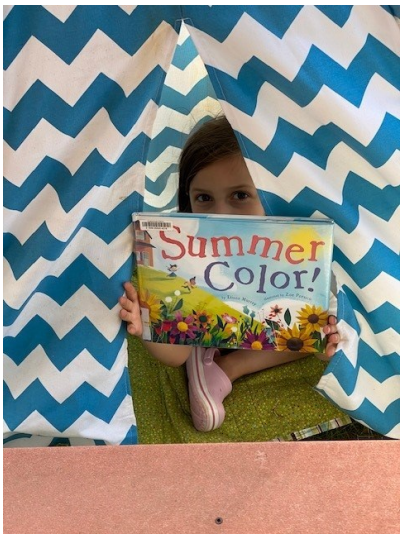
After several years of rainy, cool summer weekends, we are finally enjoying summer, even if it's hot, weather! My gardens are thriving; the tomatoes, beans and cucumbers are lush and green. Even the peppers have a few little pods!

The hydrangeas that I complained about last year when they only had 3-5 blooms are over-producing! We can hardly get up the walkway!

The grandkids got out of school, but with summer reading, which they loved! They received Olympic BINGO cards where they can earn medals for completing one line, three lines or the whole board. You know what they are going for!

Squares didn't include only book subjects; they also "Read a book in a tent," and "Read a book with "Summer in the title."

The kids got 3 squares completed in one reading outside (another square) by reading in a Teepee that my brother, Eric, gave them years ago.



If your summer includes traveling, we want to remind you: ***Hackers do not take a vacation,*** and they are excited that you may let your guard down as you unwind and forget about the challenges back home.

Last year, we put out a ***Safe Travel Guide.*** You can review it and even request a free printed copy, here: **https://actsmartit.com/travelsafe/**

Always At Your Service,

Continued from front page

- **Cyber scammers can trick employees** into sending them money or giving up confidential or sensitive information like passwords or bank information. It often starts with a phishing email, social media contact, or a call that seems to come from a trusted source — for example, a supervisor or other senior employee — that creates urgency or fear. Other emails may look like routine password update requests or other automated messages, but are actually attempts to steal your information. Scammers also use malware to lock organizations' files and hold them for ransom.

4. Treat your email like the valuable asset that it is to your business.

Your email password must be strong and DIFFERENT from every other password that you use. If a hacker gets into any of your secured sites, the first thing they will try to do is change the password so you can't get back in. How do they do that? They request a password reset — sent to your email address. If they can get into your email, they have the keys to your kingdom and can access every account that you have.

5. Secure your mobile devices, too.

70% of internet fraud is achieved via mobile devices. The majority of all internet traffic comes from mobile devices. Hackers recognize this, and they're able to commit cybercrimes with them as well. Keep apps to a minimum to keep the threat of malicious apps low. If possible, only use company owned smart phones to maintain control and security.

6. Cybersecurity Awareness Training for Everyone!

Human error is the biggest threat to cybersecurity Cybersecurity training makes your business more secure. Cybersecurity training may be required for your industry's compliance regulations Training that is interesting, interactive and fun will be more effective The owner and/or management must be invested as well. And don't use training as a punishment, or it will always be resented.

7. When an employee leaves…

Many businesses don't think past getting back the keys when an employee leaves, whether by choice or not. It is important to make sure that they are disconnected from all access to company files and data. Remove access to email; forward it to another employee for 1-6 months so nothing is missed.

Change all passwords, especially if they shared them with others. Remove references to them from all company documents, including your website and voice mail Contact your IT provider to be sure they know not to allow access.

Is Working on Your Smartphone a Risky Business or

The increasing use of mobile devices in our personal lives has led to a growing acceptance of smartphone usage at work.

As a result, the boundaries between our private and our employer's digital domains have become blurred.

While a few employers are reluctant about working on personal smartphones, for many industries it has become normal for employees to be responsive online – answering calls and emails through their mobile devices. And, while the positives and negatives of this can be debated, it can't be denied that this has created a secondary issue: a rise in cybercrime targeting mobile devices at work.

Here, we take a look at how mobile services have become a major cybersecurity risk for businesses, and some effective tools to help solve these issues, and safeguard your company's private data.

USE OF MOBILE DEVICES FOR BUSINESS

It is well known that mobile devices have become far more common in the work environment over recent years. Once considered a no-no in the workplace, mobile devices are now extremely common. In fact, 87% of companies say that they expect staff to use personal devices for work purposes.

There are significant positives from this perspective too, as 75% of employees say that using their smartphone makes them more productive at work. It can be easy to understand how this can feel like a win-win scenario. Companies want them to be used, and employees want to use them. However, businesses need to be aware of the greater exposure to cybersecurity attacks this presents – an important fact that is often overlooked.

MOBILES NEED PROTECTIVE MEASURES

Employees who use computers at work are generally protected by a range of cybersecurity measures. Smaller businesses and those less security orientated will almost always still have measures such as a firewall and anti-virus software that runs across all the machines in the system. Larger and more advanced businesses might also have cybersecurity software for their computer systems, such as SIEM and MDR.

However, what these services all have in common is that they do not provide protection for personal devices, smartphones, or regular mobile internet use, which must also be a consideration. Remember, smartphones that are not considered a part of the company IT infrastructure may still be able to access and leak sensitive company information but lack these powerful cybersecurity measures to keep them safe.

What your business can do

It may be that your business simply hasn't caught up to the fact that more workers are using mobile devices and a variety of endpoints. It is important to create a mobile-device policy and establish a formal code of conduct so that staff understand, and are fully aware of the current cyber threats and their company's vulnerabilities.

Staff also need to take responsibility for their own mobile phone cybersecurity. Teach them how to keep devices secure by using strong passwords and antivirus software, for example, as well as taking precautions if they are working in public places and surfing between work and home networks.

Are You Cybersecure?

MOBILE MALWARE ATTACKS ARE ON THE INCREASE

Once something becomes common, you can be sure that cybercriminals will look for ways to exploit it. This has certainly been the case with regards to the use of mobile devices within a business setting.

A recent report revealed that mobile malware attacks rose by 15% in 2020, and given that this number has been growing for a number of years, this represents a serious problem. Malware – once something we only generally worried about in computers – has become increasingly common on mobiles.

Malware can be extremely troublesome, not least because it can actually stay on a device for a very long time without being noticed. This means that cybercriminals can breach a system and steal data for a significant period after malware has been implanted on the device.

What your business can do

When it comes to malware, by far the most common factor in what leads to a cyber attack is human error. As such, businesses need to provide high-quality cybersecurity training sessions to staff. Make sure that these sessions are regularly updated.

REDUCE THE RISK OF WORKING FROM HOME

As a part of the COVID-19 pandemic, there has been a huge rise in the number of people working from home. That's been very good news from a number of perspectives; productivity and staff morale have gone in a positive direction. But from a cybersecurity perspective, home working is something of a challenge.

"With remote working the new norm, it's easy to slip into bad habits," says Juliette Hudson, Senior SOC Analyst at Redscan. "However, with cybersecurity risks being greater than ever and remote workers lacking office protections, it's important to maintain a high, if not higher, standard of security awareness."

It is common for private computers to have reasonable cybersecurity measures, but actually relatively rare for mobile devices. This means that if more people are working at home and using mobile devices, they are potentially causing cybersecurity issues for the business they work for.

What your business can do

Look out for the issue of shadow IT. Shadow IT refers to apps and software that are used on devices without the IT knowing about it. Typically, the IT team will check and approve all applications and software being used by staff. But if these applications are on mobile devices that the IT does not have access to, it can lead to corrupted software or applications with known vulnerabilities being used inadvertently. These can be exploited by cybercriminals.

ENDPOINTS ARE A MAJOR TARGET

While businesses can be targeted in many different ways, there has been a significant rise in the specific targeting of endpoints. If cybercriminals are able to gain access to an endpoint – such as a mobile device – they can get into the system as a whole.

This is something that many businesses still are not putting in the right level of effort and investment on.

What your business can do

It's a great idea to limit access. In the past it may have been acceptable for all members of staff to have full access to company data via their logins. But in an era where we need to be more careful, it makes sense to limit staff members so that they only have access to the data they need for their job.

This way, if a mobile device is compromised, it alone will not give a cybercriminal complete access to the company files.

Mobile devices have an important role to play for businesses – they are liked by employees, and it is clear that they have naturally become important to how companies operate. But as they pose a cybersecurity risk, more has to be done to integrate a more holistic cybersecurity policy that puts a greater emphasis on ensuring mobile devices are secured in the same way as other machines utilizing the system.

https://staysafeonline.org/resources/is-working-on-your-smartphone-a-risky-business-or-are-you-cybersecure/

In our last edition we reviewed a few different scams and some tips on ways you can protect yourself and what to do if you think you were the victim of a scam.

If you missed our first alert, just stop by our East Wareham branch and we'll give you a copy

It is more important than ever to make sure that you are aware of the many scams fraudsters are trying to get away with. This mont, we are going to review a different type of scam and what you can do to protect yourself if you believe you are being scammed, or have been a scam victim.

One of the more common scams that we are seeing almost once per week is the "Advertisement for Sale" scam. This scam is very common on nearly any website someone can advertise something for sale.

Some very common websites we see this from are Facebook, Craigslist, Offerup, sometimes we even see these on websites for rental properties.

The way this scam works is you may be browsing Facebook Marketplace for a specific item, let's say a new boat. You found someone selling a boat but the deal just looks a little bit TOO good to be true. The scammers know that an attractive price will bring in more possible people to scam.

The most important thing to be careful of is if anyone selling a product wants you to send money via Venmo, Zelle, or Cashapp. These apps send your hard earned money electronically and the funds leave your account instantaneously.

Part of the agreement to use these applications indicates that you are solely responsible for any transactions that are sent and there is ZERO recourse if you hit that send button. Once you send the funds to the scammer, they will no longer answer you, they will block your number, or even worse completely disconnect the original number you were communicating with. They use a fake name, and fake profile to stay under the radar. You are out your money and you definitely aren't going to get the boat.

How can you protect yourself from this scam? To start, if you are buying an item from a third party online it's very important to make sure this is a legitimate person. It sounds silly but look at their Facebook, do they have a lot of friends? If they are selling the item locally, do they have any friends locally?

These are big red flags, as scammers will typically create a new account to do a new scam. Another great tip is to NOT send any money until you can see the item you are buying, make sure you can verify that the item physically exists.

My final tip, which is the most important… Never ever send a Zelle, Venmo, or Cashapp to someone you do not 100% know and trust. These apps can be very helpful, but only with people you know, they are easy methods for fraudsters to get funds!

Vincent A Pircio, Branch Manager II,

Rockland Trust

2995 Cranberry Highway, East Wareham, MA 02538

Phone (508) 295-6900 | Fax (508) 295-7178

Vincent.Pircio@RocklandTrust.com

* IMPORTANT DEPARTMENT OF LABOR AND EEOC UPDATES *

Changes regarding non-exempt and exempt minimum salary threshold

BEGINNING July 1, 2024, the US Department of Labor's (DOL) final rule to the Fair Labor Standards Act (FLSA) increases the minimum salary threshold for overtime eligibility for most salaried workers. Most salaried workers who earn less than $43,888 annually will be eligible for overtime. That reflects a change in the exempt classification from $684 to $844 per week. The overtime exemption amount will increase again on JANUARY 1, 2025, to $58,656 annually ($1,128 per week).

New EEOC definitions resulting in the need to review and update anti-harassment and anti-discrimination policies

The agency's guidance addresses some new topics, such as "misgendering", and also notes "outing" an individual as potential harassment. In terms of definitions, national origin harassment now includes *cultural and linguistic* characteristics while race harassment has been expanded to include protections extending to *name, cultural dress and hair style* linked to a person's race. The guidance further clarifies "associational harassment". With regard to liability, the EEOC recognizes an employer's defense to hostile environment claims where the employer takes prompt remedial action to correct and prevent further such harassment.

Attorney Helene Horn Figman combines specialized legal knowledge in employment law with the skills and perspectives uniquely suited to Human Resources Consulting. www.figmanlaw.com

Information about her anti-harassment and anti-discrimination education programs can be found at www.workplaceawarenesstraining.com

This article has been prepared by the Law Offices of Helene Horn Figman, P.C. for general informational purposes only. It does not constitute legal advice and is presented without any representation of warranty whatsoever.

Helene Horn Figman

Law Offices of Helene Horn Figman, P.C.

Employment Law & HR Resource Management

45 Bristol Drive Suite 207, South Easton, MA 02375

FigmanLaw.com hfigman@figmanlaw.com

508-238-2700

ACTSmart IT
332 Main Street
Wareham, MA 02571

www.ACTSmartIT.com

In This Issue:

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
508 272-5120
SusanR@GrammarGoddess.com

Every month, we craft a captivating infographic on a topic that piques everyone's interest.
Dive into our collection or request previous editions at *ACTSmartIT.com/infographics*.
And the best part? We'll print and mail them to you for FREE!