The Tech chronicle

Sharkbot

Malware was found in several Android Antivirus apps.
If you own an Android device, odds are excellent that your go-to-source for apps of any kind is the Google Play Store.
Sadly, hackers know this and they are always looking for new ways of attacking.
Recently, six different apps were found to be poisoned with variants containing the Sharkbot malware.
Sharkbot is designed to steal usernames and passwords by displaying windows that appear legitimate.
Read our April 30th blog.

May 2022

This monthly publication provided courtesy of Carlos Soto. Franchise owner since 2005.

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Keep Your Business Compliant
By Following These Tips

Compliance is incredibly important for any business. A failure to remain compliant can spell doom for any business, regardless of size. Being compliant is the act of following certain established rules, regulations, laws and guidelines. But what many business owners don't realize is that compliance and security go hand in hand. Compliance is in place to prevent security breaches and give guidelines for what to do if a breach does occur.

Your company won't become compliant on its own, though. It often takes plenty of time, effort and money to ensure that your business stays compliant, especially given how rapidly technology advances. Twenty-five years ago, you wouldn't have had to worry about many of the issues that plague business owners these days because the Internet was nowhere near as developed as it is now.

But times have changed, and your business has to change with it or you will fall victim to cyber-attacks. Before you spend time and money trying to figure out if your business is compliant or not, you should ask yourself some questions.

- Does my business have antivirus software and is my network protected by a firewall?

- What data is my business encrypting?

- Do I have a system in place to manage network-connected devices?

- Are there disaster recovery plans in place, and do I use backup solutions?

- Is there a business continuity strategy?

- Do I have employee training in regard to security?

After you've answered these questions, you'll have a better idea of what needs to be done to ensure your business stays compliant. You may be thinking you need to rush out and buy the necessary technology and equipment to fill any holes, but you should focus on your team more than anything else.

According to a study by IBM, 95% of cyber security breaches stem from human error. We've talked at length about the importance of training your employees to be cyber-secure, but the reality is that employees who have not bought into a cyber-secure culture are putting your business at risk. You must have some type of employee training in place so they can learn all they can about cyber security and keeping your business protected. Without proper training, you cannot expect your employees to be inherently cyber-secure.

After you've fully trained your employees, you can put more focus into bringing in the proper technology and equipment to plug any lapses in your compliance plan. If you don't have antivirus software or firewalls, you should invest in them before anything else. Once those are in place, you can focus on a few specific pieces of technology to make your business more compliant.

One of the best investments you can make is to put an e-mail spam filter in place. Though your employees will

95% of cyber security breaches stem from human error.

be trained and hopefully well-versed in cyber security, mistakes can still happen. E-mail-based phishing attacks are one of the easiest ways for a cybercriminal to gain access to your company's valuable information. All it takes is one click on the wrong link to compromise the entire network. With a filter, you won't have to worry about your employees accidentally clicking on a sketchy e-mail because it will never make it to their mailbox in the first place.

Additionally, you should also introduce strong security password practices as well as multifactor authentication. Part of your training for your employees should include tips and strategies for creating strong passwords. Oftentimes, people will use the same passwords for every account, which can leave your business vulnerable if one of their other accounts is compromised. Multifactor authentication takes this step to the next level since your employees will also receive a text message authorizing their login into their e-mail or other accounts. It's a simple way to ensure your bases are covered.

Staying compliant is an extremely important part of your business. It helps protect you and everyone who works for, or does business with, your company. However, it takes time to put these practices into place. If you feel like you don't have time to get your cyber security measures in place or if you simply need more information about managed services providers, give us a call. We would be glad to help you with your cyber security or compliance needs.

Get More Free Tips, Tools and Services At Our Website
www.ctmaryland.com or call 240-399-9600

We got your back

Recently, we were working with one of our valued clients. We have been helping them for years and we have gotten to know their business as well as their practice well.

Recently, we noticed that they were being charged for a service that, after a little investigating, they were not receiving.

We alerted the owners and pointed out that they had been paying for non existent services that were to be installed, but never had been completed fully.

This had been going on unnoticed for over three years. And not once had the vendor reached out to the client to inform them of this.

After a quick calculation, we found that they had paid over $118,000.00 for nothing. We understand that they contacted the vendor after our meeting and they are going to be receiving a refund of that money.

We, at Computer Troubleshooters, don't just fix computers. We like to invest time in getting to know our clients so that when something doesn't quite sit right, we will investigate.

In this case, we were able to help the client in finding an opportunity for getting a substantial refund.

Let us help you, do better.

5 Tips To Spot Candidates With The Right And Wrong Stuff

I recently had the opportunity to sit down with Carter Cast, the author behind *The Right – And Wrong – Stuff: How Brilliant Careers Are Made And Unmade.* Hiring success has a great influence on career success, and we discussed five negative archetypes that confront employers while filling a job opening. Together, we discovered some telltale signs that your interviewee may fall into one of these categories.

Captain Fantastic
While it might seem like "Captain Fantastic" would be a vital part of your team, they often cause division. Someone who is a Captain Fantastic is usually overambitious and has no qualms about stepping on others to get ahead. If you're interviewing a candidate and they mention that their greatest accomplishments revolve around beating others rather than delivering value or developing teams, you probably have a Captain Fantastic on your hands.

Solo Flier
Have you ever worked with someone who thinks their way is the best and only way to do something? It's very frustrating. While this type works well individually, they can be detrimental to a team environment. They usually claim to have no time or were too busy to accomplish their tasks; in reality, they may fail to hire and delegate properly. I've met with many people who fit this category and end up leaving their job due to burnout after taking on too much work.

Version 1.0
Change is a necessity in the workplace, but sometimes people prefer to stick to their routines. To spot these people in interviews, listen to their stories and pay attention if they mention changes in the workplace and how they responded. If they stayed on the same path, that's a red flag. I knew a manufacturing executive who failed to adapt to new technologies. This caused him to lose some of his biggest clients, and the business fell into a tailspin.

The One-Trick Pony
These people usually get stuck in a rut because they rely on their greatest strength to solve *all* problems. They will often aim for lateral moves rather than trying to broaden their horizons. I interviewed a one-trick pony recently who wrote amazing copy but struggled when meeting with clients in person. His communication skills weren't strong enough to work with clients or lead large teams. His career became stagnant even though he was eager to grow and move up.

Whirling Dervish
Energetic employees improve morale and production in a workplace but sometimes lack the follow-through needed to complete projects. You can usually spot these people in interviews if you notice them avoiding your questions. They often come up with excuses for why they didn't achieve results. Great ideas and strong morale do not make up for a lack of completion.

With knowledge of these archetypes, you can avoid hiring the wrong candidate for your team and instead focus on finding the perfect fit.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best-sellers. He stays active in his community and has advised many government officials.

◼ How The Pandemic Impacted Online Grocery Delivery Companies

After taking a trip to go apple-picking in Lancaster, Pennsylvania, Abhi Ramesh came up with an idea to prevent food waste. He saw apples all around the ground that would eventually be thrown out. He thought there must be a better way and began developing his company, Misfits Market. They offered a subscription service and single-order boxes of "unwanted" produce.

When the pandemic hit, Misfits Market had to completely revolutionize the way they operated. They saw five times as many orders and had to shut down their website's checkout page while they figured out a plan to meet the demand. They created a wait list while hiring a massive number of new employees. Their staff grew from 175 to over 1,000 in a few short months. Their plan

seems to have worked out, as Misfits Market is now valued at $2 billion and has expanded its delivery service to include items not considered produce.

◼ 3 Ways To Cut Your Company's Energy Bills

Some of the biggest costs that brick-and-mortar businesses face are gas and electricity bills. However, you can't just cut these energy bills out of your budget; they're essential to your business. That doesn't mean you should be stuck paying incredibly high bills, though. There are things you can do to lower your company's monthly energy costs.

- Get an energy audit and find out exactly what is driving your bills up. You can look online for checklists and templates to get you started.

- Update any old or outdated technology from your office equipment to the break room.

Older technology can produce higher energy costs.

- Involve your team by informing them of the importance of energy conservation. You need to have everyone in your business working to keep energy costs down.

◼ Improve Your IT Security By Making IT Part Of Your Company's Culture

Many business owners who are trying to improve their company's IT security look at fixing potential hardware and software problems. No matter how many holes owners fill or barriers they put up, hackers can still find their way to important information. The simple truth of the matter is that you cannot single-handedly control and monitor your business for security risks. You must ensure that your entire team is on board and dedicated to maintaining a secure culture in the workplace.

Start with the top and make sure your leadership team has bought into the culture. They'll help influence the rest of the team. You also need to incorporate IT security training into your onboarding process. This will ensure that everyone who is hired understands the expectation. Continue this training with your current employees by having an annual refresher training. If your team buys into the security culture, you will have much less to worry about.

Scams and more Scams
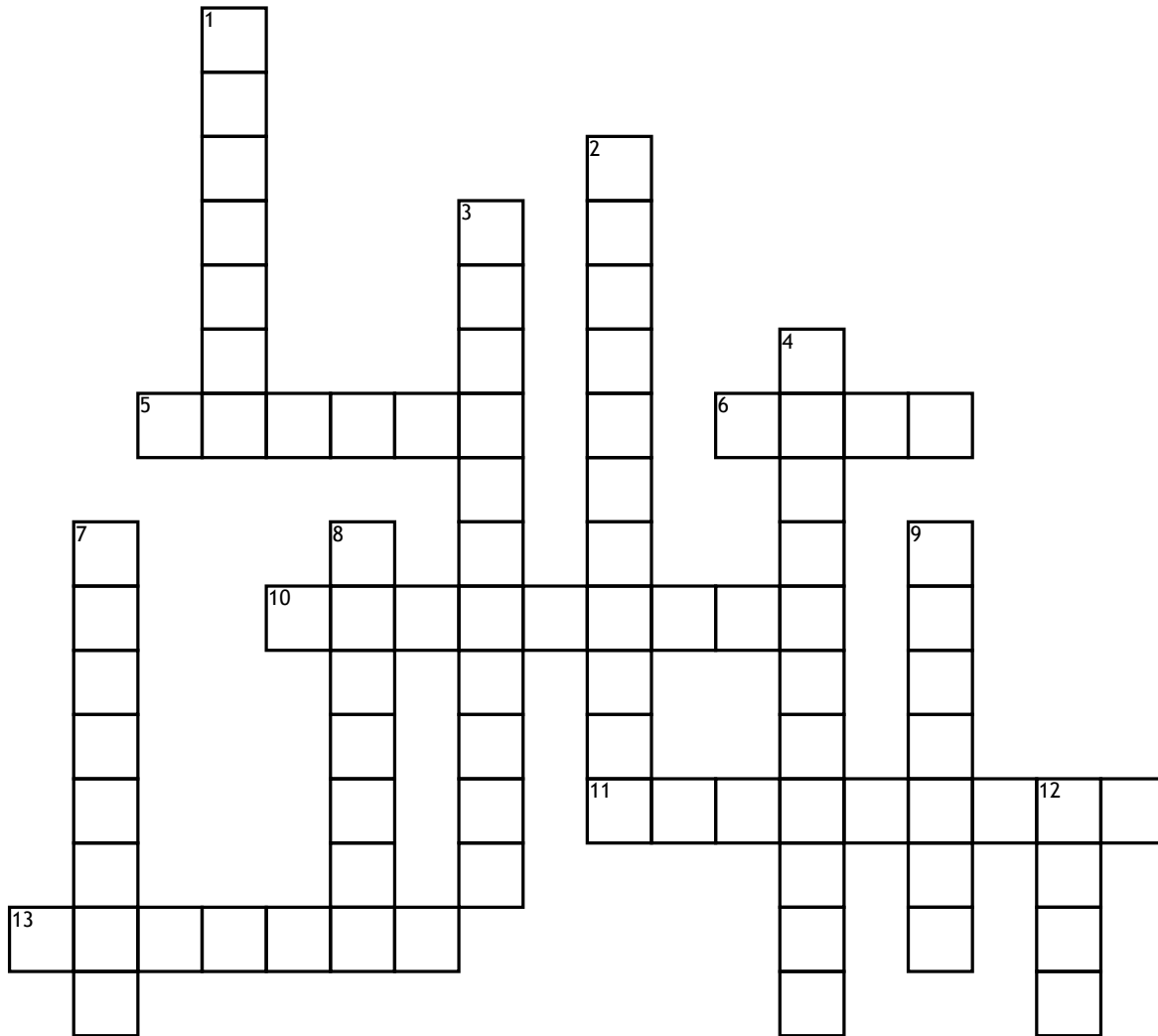
Across

5. You should _____ a phone call when you don't recognize the caller

6. You may receive a _____ message from an unknown number that includes a link

10. Calls have people's phones ringing nonstop with increasingly natural-sounding recorded voices

11. You should be _____ when someone contacts you asking for information

13. A touchless option to do things like read a menu or make payments electronically

Down

1. Voice Phishing is called _____ and is a form or fraud that uses phone calls and voicemails to trick victims

2. You get a call, email or text claiming that you won a prize but must pay an up-front fee is called a _____ scam

3. Scammers _____ IRS personnel, police, survey takes, delivery people to gain your trust

4. ____ _____ scams start with a popup or warning that you are infected. Normally you have to make a phone call

7. A type of scam that involves scamming medical benefits

8. While _____ scams are not new, they continue to rise to the cost of $547 million in 2021

9. A _____ scam persuade victims to send money for a fake cause

12. Software that may steal information from your phone after you install it

Right Now Cyber Criminals, Hackers And Thieves Are Either:

A Planning To Steal Your Company Data, Financials And Customer Information

B Have Already Infiltrated Your Company And HOPE YOU DON'T FIND OUT!

C (There Is NO Option C.)

There's a new saying in IT: "It's not a matter of IF you'll have a data breach, but WHEN." No matter the cyber force field you may THINK your IT team has in place, these expert hackers and cyber criminals ALWAYS BREAK IN.

Don't believe us, just ask these tiny, little companies:

Yahoo - 3,000,000,000 user accounts compromised
Equifax - 143,000,000 accounts compromised
JPMorgan Chase - 76,000,000 households hacked
Target - 110,000,000 people victimized
Uber - 57,000,000 users and 600,000 drivers exposed

Get The Peace of Mind That Your Credentials, Company Financials and Customer Records are 100% SAFE!

Claim Your FREE Company-Wide Dark Web Scan Today!

Get a Full Report — Good or Bad — In Just 24-48 Hours!

Go To: https://go.ctmaryland.com/dark-web-scan and fill out the form.
Or Call: 240-399-9600

Please Note: This FREE and Confidential Dark Web Scan is a one-time offer exclusively for you from Computer Troubleshooters Maryland

Offer Expires 05/31/2022