The Tech Chronicle

Apple Malware

No, it's no joke. Apple has long since been considered a mostly virus-free system.

But times have changed, we have documented clients over the years who have had viruses and malware attack their computer and reached out for us to help them out.

Now that Apple has a great foothold in the market, the increase in malware for Apple systems have been increasing since 2015 and it just keeps on growing more and more.

Read our January 23rd, blog.

February 2021

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.

How To Enable Remote Work Without Exposing Your Entire Business To Cybercriminals

A record number of businesses said goodbye to the traditional in-office work model in 2020. They embraced the remote work model as they adapted to the new COVID-19 reality. It was a huge shift that came with many challenges, and some of those challenges are still felt today.

One of those challenges was – and is – cyber security. Businesses wanted to get their remote workforce up and running, but there were a lot of questions about how they would keep their newly remote employees secure.

So, how can you enable remote work while keeping your business and your employees secure? How do you keep cybercriminals out? The answer is multifaceted. There is no one-size-fits-all approach to cyber security — that would make things much easier! But there are several steps you can take to help your remote team stay productive while keeping the cybercriminals out. Here are three things you need to do:

1. Skip the public WiFi. This is Cyber Security 101. Never use unsecured, public WiFi, especially when working. For remote employees who have the option to work from anywhere, using public WiFi is tempting. It's just so easy to access, but it comes with huge risks, including the potential to expose your device to intruders.

Thankfully, there are plenty of options to help keep employees connected without having to worry about snoops. The most popular is the VPN, or virtual private network. VPNs allow remote workers to securely access the Internet, even through public WiFi. VPNs are ideal for remote workers who need to routinely access your network.

Another option is the personal hotspot. This is a portable WiFi access point, usually

paired with data service through a telecom like Verizon, AT&T or T-Mobile. It gives remote workers flexibility to work anywhere they can get high-speed data service. Because the remote worker is the only person on the hotspot (and should be the only person), there is less worry about hackers snooping for your data.

2. Have a strong device policy. When it comes to cost-cutting, it can be appealing to let employees use their own devices while working remotely. Avoid this, if possible. The bring-your-own-device (BYOD) approach has its benefits, including keeping costs down, but the security costs could be massive, especially if an employee gets hacked or misplaces crucial data. In short, BYOD can get complicated fast, especially for businesses unfamiliar with the BYOD approach.

That said, many businesses work with an IT services company or managed services provider to create a list of approved devices (PCs, laptops, tablets, smartphones, etc.) that employees can use. Then those devices are loaded up with malware protection, a VPN, and other security solutions. So, while employees may be using a variety of devices, they all have the same security and other necessary software in order to perform their duties.

The best device policy, however, is to provide employees with

> **"There is no one-size-fits-all approach to cyber security — that would make things much easier!"**

work devices. This ensures that everyone is using the same hardware and software, and this makes it much easier to keep everyone up-to-date and secure. It takes a little more effort logistically, and it has a higher up-front cost, but when it comes to keeping your business secure, it's worth it.

3. Don't forget about physical security. While a lot of businesses are focusing on digital security right now, they're not putting a similar focus on physical security. They may have a team of people working remotely spread across different neighborhoods, towns, states or countries. This mobility comes with the risk of device theft or loss.

If employees will be carrying their work devices with them for any reason, those devices should be kept nearby at all times. That means *never* leaving work devices in vehicles or unattended at a café or airport (or any location). Never leave a device where it has the potential to be taken.

It's also important to remind employees to not only keep their doors locked but also keep work devices out of sight. You wouldn't want to set up a home office in a room facing the street outside while leaving the windows open and the door unlocked, because you never know who may walk or drive by. Just as cybercriminals are always looking for ways to break into your network, criminals are looking for opportunities to walk away with high-value items.

The way we work is changing, so we must be prepared for whatever happens next. Implementing these three steps will give you a starting point, but they aren't the end point. Work with an experienced MSP to get the most out of your remote work approach. Many businesses will not be returning to the traditional in-office model, so the more steps we take to secure our businesses and our remote teams, the better off we'll all be.

Babuk Locker

What is that and why should I care? A new ransomware strain has been found attacking corporate networks? Corporate networks? Again, why should I care for my small company or my home computer systems?

Because when you think about how you can connect to anyplace in the world, look at the fact that every place in the world can connect to you just as easily.

Granted, if you are ransomed by the Babuk Locker, it won't be very expensive because it's only between $60,000 and $85,000 USD. Not much considering that the average ransom demand last year was around $110,000 USD.

The fact remains that keeping systems secure is everyone's business because it affects us all.

How secure are your computers both at home as well as at work?

Consider this, working from home allows you to, work from home. But you are also connecting to your secure work computers from an unsecure home network.

You could be part of the weakest link just begging to get breeched.

Read out January 14th blog on the website for more information.

Communication In Times Of Fatigue

In light of all the Zoom and videoconferencing meetings, communication is changing both internally and externally.

Some companies think working remotely is the best thing they've ever done, while others say it's awful because they thrive on personal, face-to-face relationships.

Oftentimes, dominant personalities can overrun the room in person, but on a video call, the indirectness of virtual communication can help more soft-spoken team members feel comfortable speaking up.

When companies are together in person, they grab a coffee and a meeting breaks out, but when you have that on video it's awkward. There has to be more structure to the meetings because people don't want to spend an excessive amount of time like they would in person. They want to make it as short and efficient as possible.

Where people could get better is in their external messages on video chats. When you speak to your team, use a different tone. Simple things like charisma, lighting and talking *to* your audience – the things people master for TV and film – take a lot more effort than chatting with your team in person. Not having this skill is hurting some on the marketing side.

In planning for 2021, companies are running into big issues and plans may need to change.

It's time for the annual reset and the One-Page Strategic Plan (OPSP) – the gift that gives back for the next four quarters. We set our annual key initiatives – six to eight things over the next 12 months to move the business forward – but what often gets left behind is time to reset ourselves.

We need to be mindful of what we're doing with our people to keep them on track on a personal-growth level. We're all a little out of our rhythm right now, but so goes the person, so goes the business. We need to develop the *whole* person to get the best results in the new year.

Answer the question: what do you want? Don't let your logic stifle what your true goals are. Once you define it, then you can set out and figure out how to achieve it.

With upcoming changes, necessary planning and so much more, how can organizations combat the fatigue?

We must make time to take a break and step away for a moment. Set some boundaries.

It's easy for us right now to just keep working – especially working from home. You have to make yourself "go home." Do simple things, like changing your clothes after work, to turn the "work" switch off. Make yourself "commute" home. At 5 p.m., go to the store and drive back home. Give your body and mind the shift change. Honor a schedule because it is easy not to.

Chip Gallent's career has taken him through a number of C-level roles with a nonprofit, a technology development company, a publicly traded dot-com firm where he served as president and more! With an extensive background in marketing, and as a fervent entrepreneur, he's led many businesses to success. Now, as a Petra Coach, he's helping others do the same.

◼ Driving Business Success In The Age Of COVID-19

Countless businesses had to figure out how to navigate the last year. Some didn't make it, but at the same time, many thrived. Nearly a year after the pandemic began, many businesses are still trying to navigate COVID-19 repercussions. How do you drive success in 2021?

Budget Wisely. Countless businesses had a knee-jerk reaction to the pandemic. They rapidly cut costs in an effort to survive. Cutting certain areas can work. But cut the wrong area of a business, and it may be hard to recover. Some companies that put off upgrading technology during the pandemic are now paying for this costly mistake with out-of-date hardware and software that created holes in their network that are open to cybercriminals. However, if your customers didn't stick around, cutting the marketing budget is disastrous.

Embrace New Ideas. COVID-19 isn't going anywhere soon. Businesses that decided not to adapt because they thought it would blow over or it wasn't serious were put into a tough spot. Meanwhile, businesses that planned and focused on innovation were in a much better spot. When your customers' habits change, your habits need to change as well. *Forbes, Nov. 23, 2020*

◼ The Realities Of Burnout

We all feel burned out every now and again. It's the point when we feel completely exhausted with our work and need to step away. But here's a different way to think about burnout: we don't get burned out because we're working *too much*, we get burned out because we're doing too *little of what we love.*

When we do things that we're passionate about, that gives us energy and keeps us going. When our work becomes work for the sake of work, that's what drives us toward exhaustion. You may be productive, but does your productivity enrich your life in any meaningful way? To truly avoid burnout, engage in activities, projects and tasks that drive you forward and keep the passion alive. *Inc., Nov. 23, 2020*

◼ 4 Traits To Keep In Mind When Hiring

1. Value-minded. They're someone who fits in with your company culture and values. They're ready and willing to learn and grow within that culture.

2. Purpose-driven. They aren't in it just to collect a paycheck. Yes, being paid is important, but there must be drive beyond that. They have their purpose and they're working toward it.

3. Standout. There's something about them that strikes you — it could be anything from their credentials to their personality, but it's something that sticks with you in a positive way. They go the extra mile.

4. Open-minded. They're receptive to feedback and criticism and use it to grow. But more than that, they're willing to give feedback to others. They're comfortable with honesty. *Forbes, Nov. 23, 2020*

2005-2020
Thank you

Computer Troubleshooters
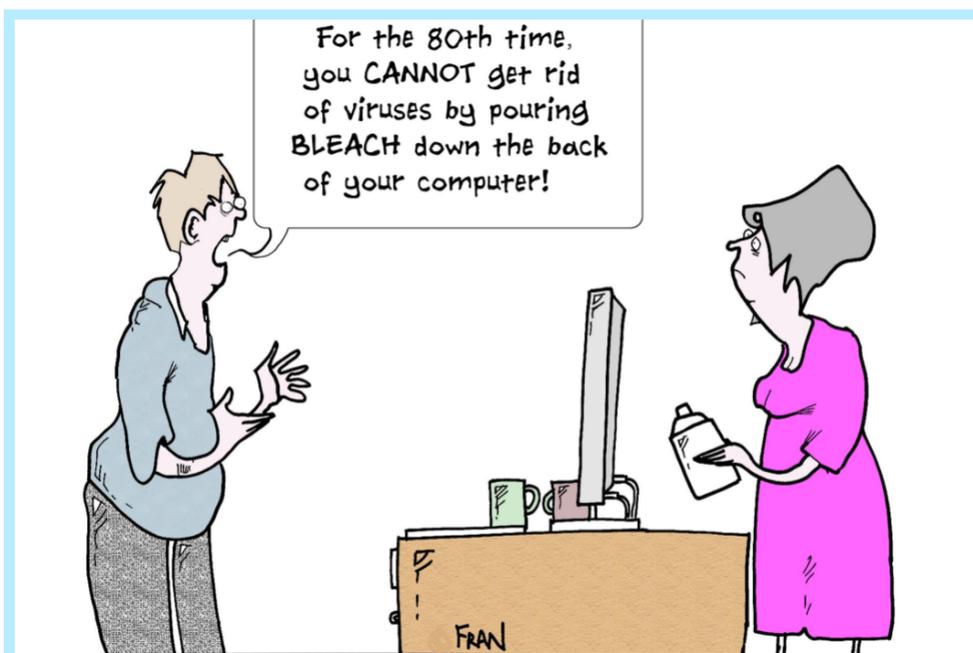
TECHNOLOGY SOLVED

15 YEARS

Name: _____   Date: _____

Who are they though?

```
W W J T R E K C E R E P S E R P J E G L W B W C
I C O H T I R E L L O H N A M R E H Q G A J D J
L T X L C T C H I J F K A D Y U G P M N L O G U
L J O H N M A U C H L Y J R F R W Y Q W A H D X
I E L M N K D J F P D S R Z A T H A J V N N E W
A A F G D Z G Q B X O E V C E T T O N D T B O Q
M L K L U J I D A K B X E J R B R C N R U A J R
S Y J Y A C O M L D J H V A J H A I M A R R O T
H L P U U C S H R B O H G S J S B X L K I D S J
O L V R Q K T O N P Z U V P A T L P Y C N E E I
C T N L W T F E P B H L E Y Y J E Q B A G E P W
K R M H Q F T E M S A K J M S K G X L P M N H A
L J R F I D R E N T I C G E T L N F I D R G J L
E V Y L M N O A L X R X K Y V D E F K I D C A T
Y A C H F I L S C W Q E O U W I S L K V W Y C E
Y T T H O A X B E V E G B U S J A W C A H K Q R
E A D A S F T I U I Z H G O T E L U A D B B U B
C N E H K C Q L J H F R L F R N G D J R V E A R
C A T K U Z G L S S T C Y L F X U R E M Y A R A
K S N R F L W G X V O N V Z I E O O Q O S S D T
U O B O P X K A P K U A B F S B D K Q M V N Z T
G F O W P P D T U Q O K E C Y O N T R E B O R A
D F J F R X P E L T B P S X B Y M X Q N H E L I
E G A B B A B S E L R A H C N N C C M G N S B N
```

BillGates   RobertMetcalfe   AlanShugart   DouglasEngelbart   RobertNoyce   JackKilby

JohnBackus   GraceHopper   WalterBrattain   JohnBardeen   WilliamShockley   JPresperEckert

JohnMauchly   CliffordBerry   BillHewlett   DavidPackard   JVAtanasoff   AlanTuring

HermanHollerith   CharlesBabbage   JosephJacquard