hAPPenings

July 2019

PIONEERING PROGRAMMERS

Protecting your business from every threat out there is close to impossible, but it doesn't have to be unmanageable. As an MSP, your primary responsibility is always to keep clients protected, which is only doable if your own systems are working adequately themselves. Remember hearing in plane safety trainings before departing that it's important to put on oxygen masks yourself before helping others in the case of an emergency? The same rule applies to this situation. Keep your systems running smoothly and only then, will you be able to provide a high level of service to your clients.

ADOPT A HIGH SECURITY POLICY AGAINST OPENING UNKNOWN EMAIL ATTACHMENTS

As an MSP, we're quick to assume that email attachments which are dangerous will be quickly filtered and destroyed by our powerful antivirus scanning technology. Unfortunately, that is almost never the case. What makes email attachments so dangerous is that even in 2019, most antivirus software and firewalls may not even be able to slightly detect whether they are infected or clean.

Sure, some email services are capable of pointing out an email attachment is potentially dangerous, but that doesn't always mean it has something on the hook. Because of this being a common statement made by the email service provider, we tend to forget about actually taking precautions against opening strange email attachments.

Having tag lines such as "you need to see this" or "open this now" makes these attachments even more threatening. How does an MSP implement a strong attachment awareness policy among its own staff? It could be scary and even embarrassing, because you expect everyone to already be aware of these simple issues. It is never a bad thing to do a refresher and bring everyone on the same page. Whether this is for clients or your own in-house setup, having a regular

session to keep your own systems safe is always a good bet to make.

How to Identify Malicious Email Attachments

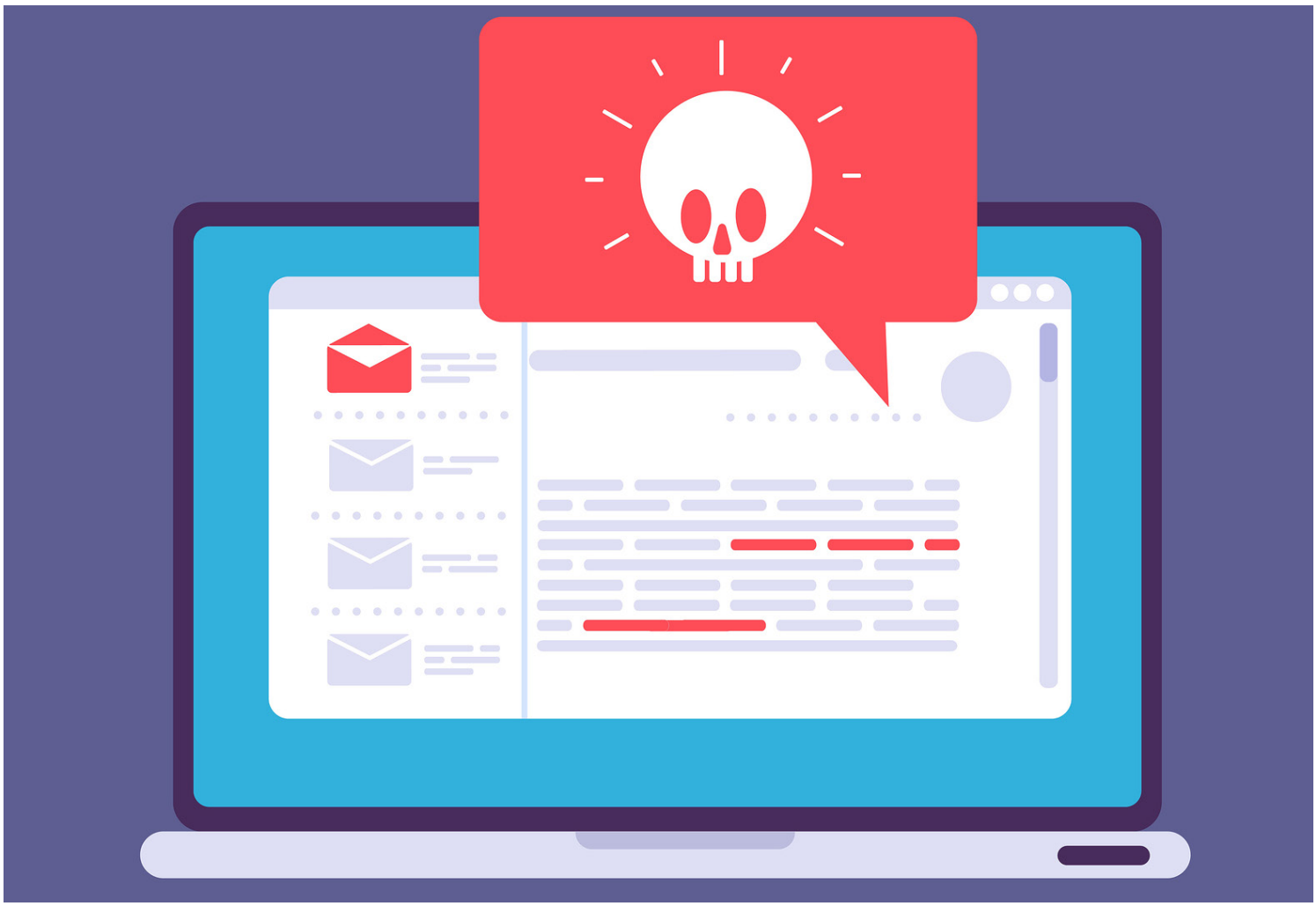
Let's state the most obvious fact first. Any email attachment which is in the form of a rar/zip file or an executable one should be looked at with serious precautionary measures in place. Most, if not all, viruses, trojan attacks, malware and ransomware attacks are done when users open and execute such files on their systems. Email services of today will be quick to notify you that this is a dangerous step to take, especially if it's from an unknown sender.

Take that advice and try to confirm at least twice what you are about to open is trustworthy or not. Never open an executable email attachment in blind faith. Many instances claim that it seemed to be from a reliable source and even passed antivirus checks but ended up being a costly mistake.

A managed service provider may even face such an embarrassment, and this could affect your clientele in the long run. Don't risk losing business just because of an email attachment.
Files with these extensions are able to not only trick SPAM filters, but also wreck havoc on your entire network setup:

- .exe – this is by far the most dangerous and notorious type of file extension which should be avoided at all costs.
- .jar – Being an executable Java application, most people are tricked into believing it is an image file due to the resemblance with .jpeg. Stay safe by avoiding running such files with this extension type.
- .cmd – Highly damaging and quick to run in the Command Prompt used by MS-DOS. This is the same as a .bat file and can be seriously harmful.

While there is a whole list of file types to avoid opening, these are the most commonly attached in emails to infiltrate a system. Keeping these on mind will help avoid most threats and should be reiterated in all of your security trainings. In-house and externally.



STEPS TO TAKE TO MITIGATE RISK DURING A CYBER ATTACK ON YOUR CLIENTS

Cyberattacks have become so widespread that the smaller ones go unreported. The massive breaches recently of Marriott Hotels and other big brand companies has smaller business owners thinking that they are safe. They firmly believe that the hackers are after only the bigger companies and that their business has nothing to worry about. This is possibly the area where most small to medium sized business owners go very, very wrong.

The difference between a larger company getting hit by a cyber attack compared to a smaller one is that the big name only has some brand value to lose. This is quickly regained as people tend to forget and move on. The SMBs of the world are unfortunately hit the hardest. They have to go through a plethora of issues which they are most likely not financially prepared to deal with.

Having a trustworthy managed service provider in the case of a security breach and hit happening can be the biggest relief for an SMB. This is why it's absolutely crucial to keep your standards updated and policies in place to help clients not only deal with a scary situation, but to also recover quickly and make a comeback.

If your client is in the business of storing personal consumer data, credit card or debit card information and any other data which may be considered of value today, extra precautionary measures should always be in place.

Backups Should be Ready to be Deployed

Losing access to corporate data and information is bound to be the first way of telling that a cyber attack has just happened. While it may not be possible to assess whether or not the attacker or attackers has gained access to that data, there is the need to always have a backup ready to be deployed to keep business running smoothly.
Risking the possibility of having complete and unrecoverable downtime can mean a significant loss in client reputation from the business side and even for the MSP managing their services.

How Strong is the Client's Physical System Security?

Attacks from within are mostly to blame after a complete audit is done and compiled about how a breach occurred. How secure are client systems and how easy is it to gain access? Many times, companies don't consider WiFi to be an issue to worry about and leave their network open to visitors and guests. This is a serious mistake which can lead to anyone wanting full access to get it without much effort.

Biometric scanners, key card-based entry and high-level wireless security all should be deployed beforehand to maximize physical security of client systems before anything else. Client data is extremely valuable and it getting into the wrong hands can be a disastrous issue for any size business.

Have Appointed Contacts for Effective Communication

In the event of a security breach, the last thing anyone wants is to figure out the appropriate person to talk to on the client and MSP end of things. Have specific representatives appointed to be focal points of contact in the situation of a cyber attack to make communicating as effective and efficient as possible. This can mean the difference between mitigating damage done or letting the attackers run loose completely.

ARE YOU SELLING DATA PROTECTION TO CLIENTS? IF NOT, WHY NOT?

In our experience, most small and medium sized business are completely over the need of hiring an in-house IT team. This opens up just so much more for them in regard to opportunities to invest that money somewhere else where it is needed. This means that they are not likely getting IT solutions from anyone else except you. Thinking that clients know each and everything about the IT infrastructure of today is a mistake many managed service providers make. In reality, your clients trust you with being their one and only. How do you live up to those expectations in actual?

If data protection services are something that you, as an MSP, offers to clients, then why are you not upselling your existing ones? Data protection isn't only a service, it is rather becoming a significant need. Without it, businesses of all sizes risk losing sensitive corporate and consumer information which could be a fatal mistake.

Not only does the lack of data protection greatly reduce the security of clients, it also opens up the opportunity for many other MSPs that may be competing for business. They can easily approach your clients and when they find out data protection is not on the table; it will be a conversation they can dominate. Don't be an MSP which loses its client base because of a simple offering that got away. Be proactive and get your clients to sign on to a highly important service.

Still wondering why selling data protection to your clients is necessary, here are some of our top reasons to get you thinking as an MSP:

Your Clients Trust you 100%

If you still can't see that your clients have signed up with you because they want you to take care of all of their IT needs, then nothing else can really be as convincing. When a business outsources its complete IT setup to another company, it hopes that the MSP will be a full service providing solution. They don't want to be worrying about not having everything that they need to conduct business without the fear of being attacked by cyber criminals.

Data breaches are scary and if data protection is not on the list of what you're doing for your clients, it may end up permanently damaging that reputation and relationship.

Competitors are Seeking out your Weaknesses

Just imaging how another MSP may be able to greatly manipulate and exaggerate the situation if they found out one of your clients wasn't getting data protection from you. This could be done in a number of ways. Either your client ends up looking for other service providers for data protection or other MSPs gain access to someone on the inside and find that information out directly from the source.

There is no telling what clients may be forced to do in that sort of situation. You shouldn't have to push them to the brink of it. Make sure you're providing a well-rounded package of services and that they don't have to look elsewhere for their needs to be met.

WHEN WAS THE LAST TIME YOU ASSESSED YOUR NETWORK'S BANDWIDTH REQUIREMENTS?

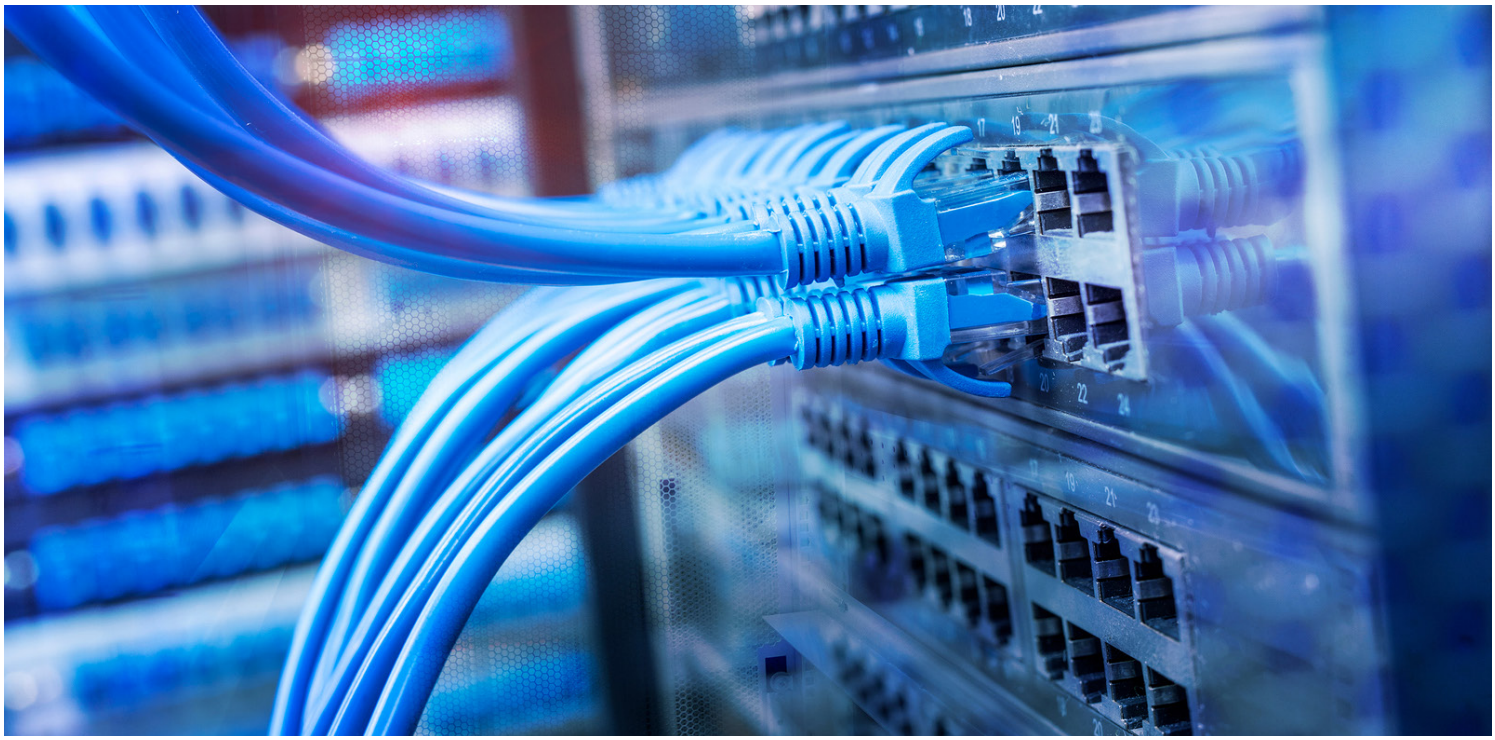
Having been around for years and helping MSPs grow their business, we've learnt that one of the biggest reasons why clients leave service providers is bandwidth problems. This may seem like a problem an MSP should not be held responsible for, but in reality, clients don't know the complete picture to the extent of being technically qualified in such aspects of business.

When they hire an MSP to take care of all of their IT needs, they literally mean ALL of their IT needs and not just a few. Those managed service providers which are regularly testing their bandwidth capacity, assessing it for future needs and making changes accordingly are seen to suffer the least loss in terms of clients moving because of this reason. This is a risk of business which can be completely wiped out and MSPs should not be losing customers ever just because of internet performance related issues.

With more and more devices being online in businesses everywhere, we also expect the speed to be faster than ever as well. Businesses are more dependent on bandwidth now, especially due to the need to constantly access cloud services and having the Internet of Things (IoT) in the equation. A ton of data is always being sent and received. This signifies the need for improved bandwidth and internet reliability.

Clients may only understand bandwidth in terms of internet speed. In reality, you are well aware that bandwidth doesn't only have to do with speed, but it is primarily the number of lanes which are open for more users to access like a smaller or larger highway. The greater the bandwidth, the more people can access a network without facing a bottleneck in transmission speeds.

If you are unable to remember when the last time you assessed your bandwidth requirements was, maybe now is the next best time to do it.



Will Low Bandwidth Impact a Business that Much?

Thinking that slower internet access may not be that bad as some say could be a horrible mistake to make as an MSP. Clients largely rely now on everything being accessible via the internet. The cloud services for their data and important corporate storage, along with now even conducting business over IP phones, instant messaging and constantly being in touch over emails. Everything now needs the internet to work efficiently and people are no longer able to cope with slow processing times.

The good thing is that fiber optic internet is now more available than it has ever been in history of the internet. This means blazing fast speeds and maximized bandwidth to have everyone online and doing everything that they want to without any hinderance. But this can also be very expensive if you just kick it up to the maximum level.

This is why it is stressed that assessing bandwidth need is important to get an accurate estimate of where your current requirements stand. Knowing this information will allow for improved investment into enhancing your bandwidth for clients while not going overboard on costs.

Need more help becoming an MSP which clients can rely on 100 percent? We're always open to helping out in even the direst of cases. Reach out to us at 972-268-9285 or book an online appointment with our MSP expert Mark right now!

PIONEERING PROGRAMMERS

www.devs4msps.com
www.pioneeringprogrammers.com

1059 S Sherman Street
#140 Richardson, Texas, TX 75081

info@devs4msps.com

972-895-3100