AUGUST 2022

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

Who else is sick of spam?

For business owners, spam is bad news.

Not only is it annoying, but it's also eating up hours of your team's time each year. In fact, it's estimated that people who get more than a hundred emails every day could be losing around 80 hours of their time each year, sorting out spam.

As well as the impact on productivity, have you considered how else it might be harming your business?

For example, how many of the emails that you send out – especially your marketing messages – are being marked as spam?

Spam filters give each email a score based on the sender reputation, domain name and many other factors. They also read the emails to spot common words and phrases used by spammers.

Using one "spammy" word in an email isn't a disaster in itself. But using too many can give you a higher spam score, and your message could be filtered into the spam folder.

Try not to use things like '$$$' or 'free money'. Other flagged words and phrases are more surprising – 'being a member', 'free trial', 'unlimited', and even 'amazing'.

Next time you're creating a marketing email, take a moment to consider how spammy your email could be perceived before you hit send. Staying out of the spam folder improves deliverability and open rates.

DID YOU KNOW...

paying ransomware makes you a bigger target?

Ransomware is evil. It's where your data is encrypted until you pay a ransom fee to get it back.

Many business owners say they'd pay the fee to resolve the problem quickly. But doing that can make your business an even bigger target for attacks.

80% of ransomware victims who paid up were then hit a second time by the same attackers.

Doh.

The greatest defense against ransomware is being 100% prepared. You need a working and verified backup, a ransomware resilience plan, and all the right security measures in place **BEFORE** you are attacked.

Are you blacklisting or whitelisting?

You know what it means to be blacklisted, right? (we don't mean through personal experience, of course).

Blacklisting is where you block something you don't trust. It's used to keep networks and devices safe from bad software and cyber criminals.

But there's another, safer way of doing that – and that's called whitelisting.

Rather than trying to spot and block threats, you assume everyone and everything is a threat, unless they've been whitelisted.

But which is the right approach when it comes to keeping your business data safe? This debate rages on, with many IT professionals holding different views.

Here are the main differences...

- Blacklisting blocks access to suspicious or malicious entities
- Whitelisting allows access only to approved entities
- Blacklisting's default is to allow access
- Whitelisting's default is to block access
- Blacklisting is threat-centric
- Whitelisting is trust-centric

There are pros and cons to each approach. Whilst blacklisting is a simple, low maintenance approach, it will never be comprehensive as new threats emerge daily. It's also easy to miss a threat, as cyber criminals design software to evade blacklist tools.

Whitelisting takes a stricter approach and therefore comes with a lower risk of access. But it's more complex to implement and needs more input. It's also more restrictive for people using the network and devices.

Confused? You're not alone! If you'd like to discuss which approach is best for your business, get in touch.

Q: How can I avoid being phished?

A: The best thing is treating every email with caution. If you're unsure, check the address it's been sent from, look for grammatical errors, and see if the layout looks like a normal email from that person or company. If you're unsure, don't click any link.

Q: What's an insider threat?

A: It's the name for when someone within your business gives cyber criminals access to your devices or network. Usually, it's not malicious. But it's why regularly training your team in cyber security is a must.

Business gadget of the month

If you want to upgrade your webcam without spending a lot, you can use your phone's camera. You also need a good tripod to hold it.

The Joby GripTight ONE is a great option. It's under $50, has bendy, flexible legs, magnetic feet, and is small enough to carry from home to the office.

Q: How do I choose the right backup for my data?

A: Security and reliability should be your main considerations. Get in touch and we'll tell you what we recommend.

This is how you can get in touch with us:

CALL: 888-895-5173 | EMAIL contact@computerzone.net WEBSITE: www.computerzone.net