December 2022

TechTidbit.com

brought to you by Tech Experts

2022: The Year Of Malware, Hacks And Phishing

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Much of our time this year has been spent working with our clients, making sure they're ready to fend off newly emerging cyber threats or malware strains.

So to look back at the year, we thought we'd round up what many experts agree has been the nastiest malware of 2022.

At the top of the list is Emotet. Chances are you haven't heard of it by that name, but it's a trojan that's spread by spam email. It usually looks like a genuine email with familiar branding, but it tries to persuade the recipient to click a malicious link (using language like 'your invoice' or 'payment details.'

It may also look like it's from a parcel company. This malware goes through your contact list and sends itself to family, friends, colleagues, and clients. Then it looks less like spam, because it's come from your email account.

In second position is LockBit. This is ransomware that's designed to block access to your files and systems when cyber criminals encrypt them.

They ask you to pay a ransom for the decryption key (which they often still don't hand over, even when you've paid). If you don't have a solid backup strategy, it is highly likely you'll experience data loss.

This is a targeted attack that spreads itself once it's infiltrated one device on a network. In fact, it can 'live' for weeks inside a network before the attack is launched.

In third place is Conti, another form of ransomware, and in fourth position is Qbot, a trojan designed to steal banking information and passwords.

It may all sound scary, but there's plenty you can do to give your business greater protection from these threats:

- Keep your entire network and all devices updated
- Don't download suspicious attachments or click links unless you're certain they're genuine
- Practice strong password hygiene, including multi-factor authentication, password managers, biometrics, and passkeys where available
- Give your people access to only the systems and files they need. Remove ex-employees from your network immediately
- Create and regularly check back-ups
- Educate your people regularly

We can help with all of this – just get in touch!

What To Include In A Year End Tech Review

When the year is coming to a close, it's the perfect time to plan for the future. Most businesses begin the year with the hope of growing and improving operations. Much of how a business operates depends on technology.

So, it makes sense to look to your IT for areas of optimization.

A year-end technology review provides an opportunity to look at several areas of your IT. The goal is to take time to focus on improvements you can make to boost your bottom line, as well as what tactics to take to reduce the risk of a costly cyberattack.

Small businesses that make smart use of technology are well ahead of their peers. Here are some of the ways they excel:

- Earn 2x more revenue per employee
- Experience year-over-year revenue growth nearly 4x as high
- Had an average employee growth rate over 6x as high

The bottom line is that companies that use technology well do better. They are also more secure. According to IBM, businesses that have an incident response plan reduce the costs of a data breach by 61%. Using security AI and automation can lower costs by 70%.

This year-end, take some time to do a technology review with your IT team or managed IT provider. This will set you up for success and security in the coming year.

Considerations when reviewing your technology at year end

The goal of a year-end technology review is to look at all areas of your IT infrastructure. Security, efficiency, and bottom-line considerations will be the key drivers for future initiatives.

Technology policies

When technology policies get outdated people stop following them. Review all your policies to see if any of them need updating to reflect new conditions. For example, if you now have some staff working from home make sure your device use policy reflects this.

When you update policies, let your employees know. This gives them a refresher on important information. They may have forgotten certain things since onboarding.

Disaster recovery planning

When is the last time your company did an incident response drill? Is there a list of steps for employees to follow in the case of a natural disaster or cyberattack?

Take time to look at disaster recovery planning for the new year. You should also put dates in place for preparedness drills and training in the coming months.

IT issues & pain points

You don't want to go through a big IT upgrade without considering employee pain points. Otherwise, you might miss some golden opportunities to improve staff productivity and well being.

Survey your employees on how they use technology. Ask questions about their favorite and least favorite apps. Ask what struggles they face.

Let them tell you how they feel improved technology would make their jobs better.

This, in turn, benefits your business. It can also help you target the most impactful improvements.

Privileged access & orphaned accounts

Do an audit of your privileged accounts as part of your year-end review. Over time, permissions can be misappropriated. This leaves your network at a higher risk of a major attack.

You should ensure that only those that need them have admin-level permissions. The fewer privileged accounts you have in your business tools, the lower your risk. Passwords of compromised privileged accounts open the door to major damage.

Overcoming Barriers for "Bring Your Own Device (BYOD)" Success In Your Business

Mobile devices make up about 60% of the endpoints in a company network. They also handle about 80% of the workload.

But they're often neglected when it comes to strong cybersecurity measures. This is especially true with employee-owned mobile devices.

Purchasing phones and wireless plans for staff is often out of reach financially. It can also be a pain for employees to carry around two different devices.

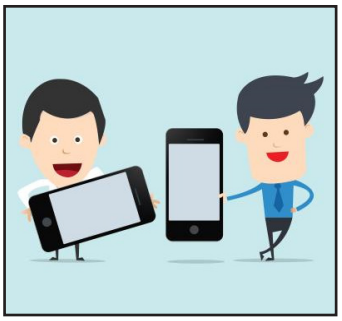
This has made BYOD the preferred way to go by about 83% of companies. Here are some tips to overcome the security and challenges of BYOD.

Define your BYOD policy

If there are no defined rules for BYOD then you can't expect the process to be secure.

Employees may leave business data unprotected. Or they may connect to public Wi-Fi and then enter their business email password, exposing it.

If you allow employees to access business data from personal devices, you need a policy. This policy



protects the company from unnecessary risk.

Keep your policy "evergreen"

As soon as a policy gets outdated, it becomes less relevant to employees. Thus, they may tend to ignore it. Make sure to update your BYOD policy regularly.

Use VoIP apps for business calls

Customers having employees' personal numbers is a problem for everyone. Employees may leave the company and no longer answer those calls. The customer may not realize why.

You can avoid the issue by using a business VoIP phone system. These services have mobile apps that employees can use. VoIP mobile apps allow employees to make and receive calls through a business number.

Create restrictions on saved company data

No matter what the type of device, you should maintain control of business data. It's a good idea to restrict the types of data that staff can store on personal devices. You should also ensure that it's backed up from those devices.

Require device updates

When employee devices are not updated or patched, they invite a data breach. Any endpoint connected to your network can enable a breach. This includes those owned by employees.

An endpoint device manager can push through automated updates. It also allows you to protect business data without intruding on employee privacy.

Include BYOD in your offboarding process

If an employee leaves your company, you need to clean their digital trail. Is the employee still receiving work email on their phone? Do they have access to company data? Are any saved company passwords on their device?

Make sure you check all this during offboarding.

SETUP CHECKLIST FOR MICROSOFT TEAMS

Microsoft Teams is a lot of things. It's a video conferencing tool, a team messaging channel, and a tool for in-app co-authoring, just to name a few.

During the pandemic, the popularity of Teams skyrocketed. You can think of Teams as a virtual office in the cloud. It's a centralized hub where teams can communicate, collaborate, and manage tasks. There is also an external communication component to Teams.

You can use the app to video conference with anyone. You can also invite guests to a chat channel.

Here are some of the features of MS Teams:

- Set Up Your Teams/ Departments
- Add Team Members
- Set Up Team Channels
- Set Up Team Tabs
- Schedule MS Teams
- Training

Contact Information

Tech Experts Support Team

(734) 240-0200

support@MyTechExperts.com

Main Office

(734) 457-5000

info@MyTechExperts.com

Sales Inquiries

(888) 457-5001

sales@MyTechExperts.com

TECH EXPERTS

15347 South Dixie Highway

Monroe, MI 48161

Tel (734) 457-5000

Fax (734) 457-4332

info@MyTechExperts.com

Insider Threats Are Getting More Dangerous

One of the most difficult types of attacks to detect are those performed by insiders.

An "insider" would be anyone that has legitimate access to your company network and data via a login or authorized connection.

Because insiders have authorized system access, they can bypass certain security defenses, including those designed to keep intruders out.

Since a logged-in user isn't seen as an intruder, those security protections aren't triggered.

A recent report by Ponemon Institute found that over the last two years insider attacks have increased by 44% and the average cost of addressing insider threats has risen by 34%

Four types of insider threats

- Malicious/Disgruntled Employee
- Careless/Negligent Employee
- 3rd Party with Access to Your Systems
- Hacker That Compromises a Password

Ways to mitigate insider threats

When hiring new employees make sure you do a thorough background check.

Malicious insiders will typically have red flags in their work history.

You want to do the same with any vendors or contractors that will have access to your systems.

Endpoint device solutions

Mobile devices now make up about 60% of the endpoints in a company. But many businesses aren't using a solution to manage device access to resources.

Put an endpoint management solution in place to monitor device access. You can also use this to safelist devices and block unauthorized devices by default.

Multi-factor authentication & password security

One of the best ways to fight credential theft is through multi-factor authentication. Hackers have a hard time getting past the second factor.

They rarely have access to a person's mobile device or FIDO security key.

Employee data security training

Training can help you mitigate the risk of a breach through carelessness.

Train employees on proper data handling and security policies governing sensitive information.

Network monitoring

Use AI-enabled threat monitoring. This allows you to detect strange behaviors as soon as they happen.

For example, someone downloading a large number of files or someone logging in from outside the country could be indicators your systems or security are compromised.

Advantages Of Conditional Access

It seems that nearly as long as passwords have been around, they've been a major source of security concern.

Eighty-one percent of security incidents happen due to stolen or weak passwords. Additionally, employees continue to neglect the basics of good cyber hygiene.

Access and identity management have become a priority for many organizations.

Once a cybercriminal gets a hold of an employee's login, they can access the account and any data that it contains. Using conditional access policies can mitigate the risk of an account breach.

What Is Conditional Access?
Conditional access is also known as contextual access. It is a method of controlling user access. You can think of it as several "if/then" statements, meaning "if" this thing is present, "then" do this.

Conditional access allows you to add many conditions to the process of user access to a system. It is typically used with MFA.

This is to improve access security without unnecessarily inconveniencing users. Some of the most common contextual factors used include the IP address that is associated with the user, the geographic location if the login, time of day, the type of device used and the role or group the user belongs to.

Implementing conditional access for identity management will improve security, automates the access management process, and allows the business to restrict certain activities.

Another advantage of conditional access is the ability to apply the principal of least privilege, making sure that users can only access appropriate resources.