Virtual DataWorks

TECH BYTES

February 2025

Stay current and secure with our monthly tech and cybersecurity updates. Discover the latest innovations, gain valuable tips, and much more!

Stay updated with the latest advancements and trends in technology.

Matthew DeWees

-President

Worried about your emails getting blacklisted? Don't worry! By maintaining clean email lists and following best practices, you can keep your sender reputation intact and ensure your messages reach your audience.

Worried about cyber threats? Our article has everything you would need to watch out for. Each poses serious risks, but with the right precautions, you can stay protected.

The truth is, what you don't know can hurt you. Your personal information could be up for grabs without you knowing, leaving you open to identity theft, financial fraud, and more.

Reach out to us at everythingit@virtualdataworks.com to schedule a chat.

Until then, stay safe,

Matthew DeWees

President - Virtual DataWorks

WHAT'S INSIDE?

DID YOU KNOW

The first computer virus, the "Creeper virus," was created in 1971. It displayed the message, "I'm the creeper, catch me if you can!" and led to the development of modern cybersecurity measures.

Virtual DataWorks

475 Wolf Ledges Parkway
Akron, Ohio 44311

virtualdataworks.com

(330) 800-2186

02 HOW BULK EMAIL CAN CAUSE BLACKLISTING

Bulk emailing can lead to blacklisting due to several factors, including high bounce rates, spam complaints, and poor list hygiene.

When email service providers detect issues such as high bounce rates, spam complaints, or poor list hygiene, they may block your emails from reaching recipients. This can significantly disrupt your communication efforts and damage your brand's reputation, as your messages fail to reach their intended audience and your credibility is undermined.

High Bounce Rates

High bounce rates occur when emails are sent to invalid addresses, harming your sender reputation and leading to your emails being flagged as spam.

Spam complaints arise when recipients mark your emails as unwanted, signaling to email providers that your messages are not welcome. This can result in your emails being filtered into spam folders or blocked entirely, reducing the effectiveness of your campaigns and damaging your brand's reputation.

To mitigate these risks, obtain explicit consent from recipients and provide clear options for unsubscribing.

Poor List Hygiene

Poor list hygiene, such as using outdated or purchased email lists, increases the likelihood of invalid addresses and uninterested recipients. Outdated lists lead to high bounce rates, while purchased lists often contain recipients who haven't opted in, resulting in more spam complaints.

This combination can significantly damage your sender reputation, leading to your emails being filtered into spam folders or blocked entirely.

To maintain good list hygiene, regularly update and clean your email lists, and ensure all recipients have explicitly opted in to receive your communications.

How To Prevent Blacklisting:

- Maintain clean and up-to-date email lists: Regularly remove invalid or inactive addresses.
- Implement double opt-in methods: Ensure subscribers genuinely want to receive your emails, reducing spam complaints.
- Monitor email metrics: Track open rates, click-through rates, and bounce rates to identify and address potential issues early.
- Segment your email lists: Personalize content to improve engagement and reduce the risk of being marked as spam.
- Follow best practices: Adhere to industry standards to protect your sender reputation and ensure your emails reach their intended audience.

03 CAN PASSWORD MANAGERS BE HACKED?

Password managers play a crucial role in keeping our online accounts safe by storing all our passwords in one secure place. They offer convenience and enhanced security, but you might wonder: are they hackable?

While no system is entirely immune to hacking, reputable password managers use strong encryption and other security measures to protect your data, making them a reliable choice for managing your passwords.

What Are Password Managers?

Password managers function like digital vaults, securely storing all your passwords in one place. You only need to remember a single master password to access them.

This simplifies the management of multiple accounts, making it much easier to handle your online security.

Can Password Managers be Hacked?

They are always on the lookout for ways to steal your information. However, breaking into a password manager is not an easy task. These tools use advanced encryption and security measures to protect your data, making it significantly more challenging for hackers to gain access.

How Can You Protect Your Password Manager?

- Choose a Strong Master Password. Use a mix of letters, numbers, and symbols.
- Enable Two-Factor Authentication. 2FA adds a layer of security.
- Keep your software up-to-date. Regular updates fix security issues and help keep your data safe from potential threats.

What Happens If a Password Manager Gets Hacked?

- Change your master password immediately to secure your accounts. This is the first and most crucial step in protecting your data.
- Decide which accounts could be affected and change their passwords as well.
- Consider shifting to another password manager if you have concerns about the security of your current one. This can provide additional peace of mind and potentially offer enhanced security features.
- Stay informed by keeping up to date with any security news related to your password manager. This will help you respond quickly to any potential threats or vulnerabilities.

Is the Use of Password Managers Worth the Risk?

- The benefits of using a password manager usually outweigh the risks. They help you create strong, unique passwords for each account.
- Choosing a reputable password manager with good reviews and security features is key. Do some research before deciding which one to use.

Take Control of Your Online Security Today!

Using a password manager will go a long way in enhancing your online security by securely storing and managing your passwords. If you need assistance in selecting the right one, we're just a contact away and ready to help.

04 BEST PRACTICES FOR SECURE DATA BACKUP

Here are some best practices for secure data backup:

- **Use Encryption:** Encryption scrambles your data, making it readable only by you. This is essential for keeping your data safe from hackers and unauthorized access.
- **Regular Backups:** Schedule regular backups to ensure that your most recent data is always protected. This can be done daily, weekly, or monthly, depending on how frequently your data changes.
- **Multiple Backup Locations:** Store backups in multiple locations to reduce the risk of data loss. For example, keep one copy on an external hard drive and another in the cloud.
- **Automated Backups:** Use automated backup solutions to minimize the risk of forgetting to back up your data. Many cloud services and backup software offer automated options.
- **Verify Backups:** Periodically check your backups to ensure they are complete and can be restored successfully. This helps you avoid unpleasant surprises when you need to recover your data.

Secure Storage: Ensure that your backup devices are stored in a secure location, protected from physical damage, theft, or unauthorized access.

- **Set Strong Passwords**: Use robust passwords for all your backup accounts and devices. Strong passwords are crucial in preventing unauthorized access and ensuring the security of your data.
- **Regularly Test Your Backups**: Regular testing ensures that your backups are functioning correctly. Periodically try restoring a file to verify that everything is in order and your data can be recovered when needed.

Take Action to Protect Your Data Today!

Don't wait until it's too late to safeguard your data. Start backing up your important files today!

By following these best practices for data backup, you can secure your valuable information. If you need assistance in setting up a secure backup system, we're here to help. Taking these steps now will give you peace of mind and protect you from potential data loss in the future.

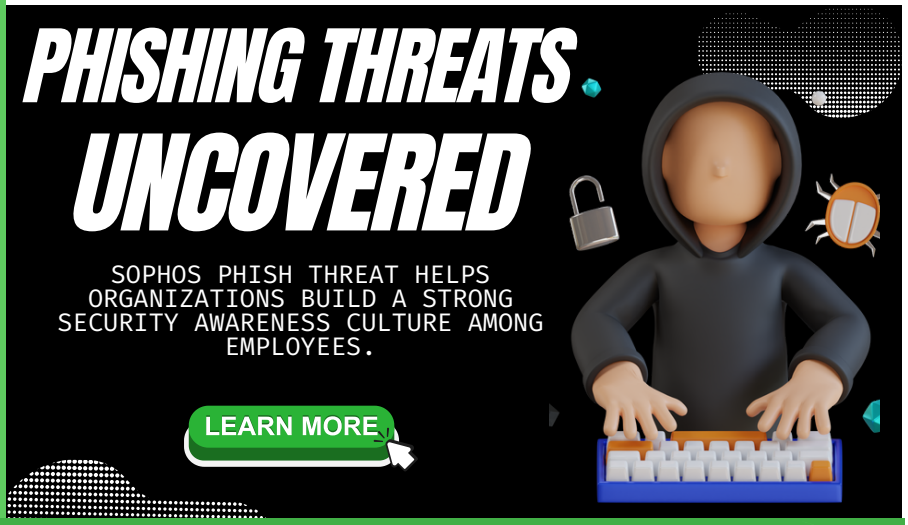
05 COMMON CYBER THREATS IN 2025

HERE ARE FIVE COMMON CYBER THREATS IN 2025:

- **Phishing Attacks**: Phishing remains a prevalent threat, where cybercriminals trick individuals into revealing sensitive information through fake emails, messages, or websites.
- **Ransomware:** This type of malware locks your files and demands payment for their release. It often spreads through unsafe downloads or email attachments12.
- **AI-driven Cyberattacks**: With advancements in AI, cybercriminals are using AI to launch more sophisticated and targeted attacks, making it harder to detect and defend against them.
- **Malware**: Malicious software designed to harm devices, steal data, or spy on activities. It can be hidden in seemingly legitimate downloads or compromised websites.
- **Cloud Security Issues**: Misconfigurations and poor practices in cloud security can lead to data breaches and unauthorized access to sensitive information.

Staying informed and taking proactive measures, like using strong passwords, enabling multi-factor authentication, and keeping software up to date, can significantly help protect against these threats. Also, be cautious of suspicious emails and links, regularly back up your data, and use reliable security software.

Do you have any specific concerns or need advice on how to stay safe online?



VIRTUAL DATAWORKS

Leveraging technology to positively impact your business!

Leading Managed Service Provider in Akron, Ohio

Virtual DataWorks, a top IT Consultant and Managed Service Provider in North East Ohio, believes technology can make or break your business. Their Managed Services program allows them to handle your IT, so you can focus on your business. Our goal is to be your trusted partner, ensuring your technology works for you.

Meet Our Executive Team

CLICK HERE