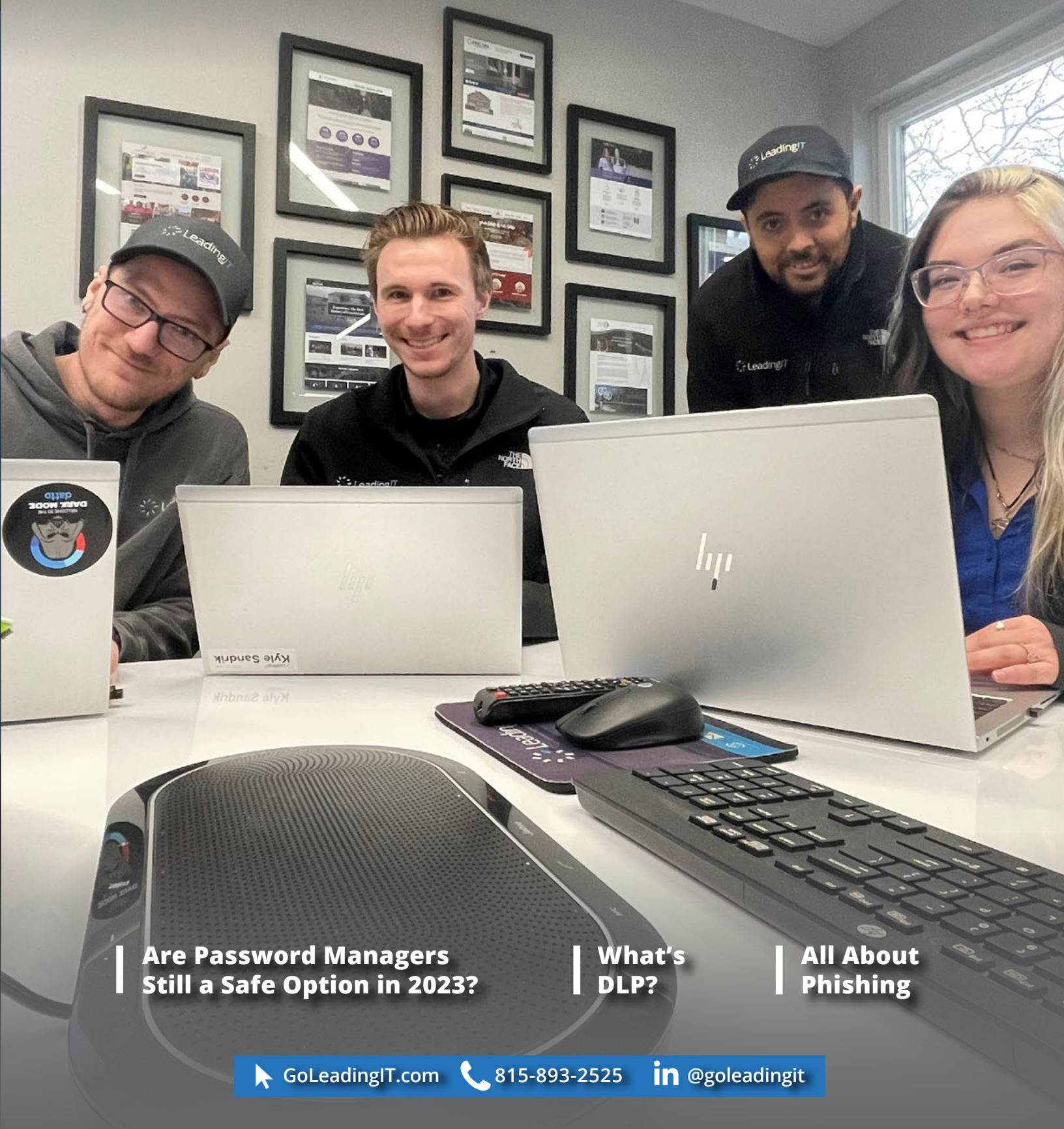
the NetWork

LeadingIT

Chicagoland CybersecurITy Support

April 2023



Are Password Managers Still a Safe Option in 2023?

What's DLP?

All About Phishing

GoLeadingIT.com 815-893-2525 @goleadingit

Are Password Managers Still a Safe Option in 2023?

Despite a steady increase surrounding cybersecurity awareness and ransomware prevention, attacks on password management systems are on the rise. The 2022 Microsoft Digital Defense Report indicated a worrisome 74% increase in password attacks. This equates to 921 attacks per second and this number doesn't seem to be slowing down any time soon.

Breaches, such as the LastPass encrypted password vault being stolen last December, have led many people to consider whether their private data is still safe with online password management systems. The short answer is yes – password managers are still a safe option in 2023, but there are some steps you should take to ensure your safety if yours gets hacked.

What Happens When a Password Manager is Hacked?

Every password manager, whether you use Bitwarden, 1Password, LastPass, or some other service, uses data encryption to keep your passwords safe. If a hacker does successfully get their hands on a system's encrypted data forms, he or she will not be able to decipher your actual password. However, the hacker may be able to see certain information specific to you such as:

- Name
- Email address
- Billing address
- Profile information

If you do find that your password manager has been compromised, there are a few safety precautions to take.

Change Account Passwords

Of course, your password manager is in place to secure passwords to multiple accounts. Regardless of the manager you choose, you will have a master password in place to access your main account. To protect your identity and profile information, change your master password to the management site.

Continue reading on page 4

What's DLP?

Data loss prevention is a set of security policies and technologies used to monitor and control how data is handled within an organization. DLP helps prevent unauthorized access, use, disclosure, modification, or destruction of sensitive information.

The main purpose of DLP is to protect your company's assets by ensuring that only authorized employees have access to them. Companies have reasons to be concerned beyond only external dangers; insiders are the cause of over 20% of security incidents. DLP protects against the transmission of private data outside of a corporation.

DLP can be used in several different ways. Here are just a few examples:

- To monitor employee activity on computers to ensure that they are only accessing files they need for work-related purposes
- To monitor Internet traffic from within an organization so that no one downloads any confidential data

Continue reading on page 4

Pictured on the cover: Jeremiah, Kyle, Salvador, Mallory

ALL ABOUT PHISHING

Phishing is a form of online fraud where the scammer uses emails, websites, or texts to impersonate legitimate businesses or people. They are designed to trick you into giving away your personal information. That's why it's important to know what phishing looks like—and how to avoid becoming a victim of this type of scam.

In a phishing attack, a criminal will send you an email or text message that looks like it's from someone you know or trust, asking for sensitive information such as your Social Security number and bank account details.

Unfortunately, phishing scams are notoriously difficult to spot — even for experienced internet users — which means these attacks can be incredibly successful.

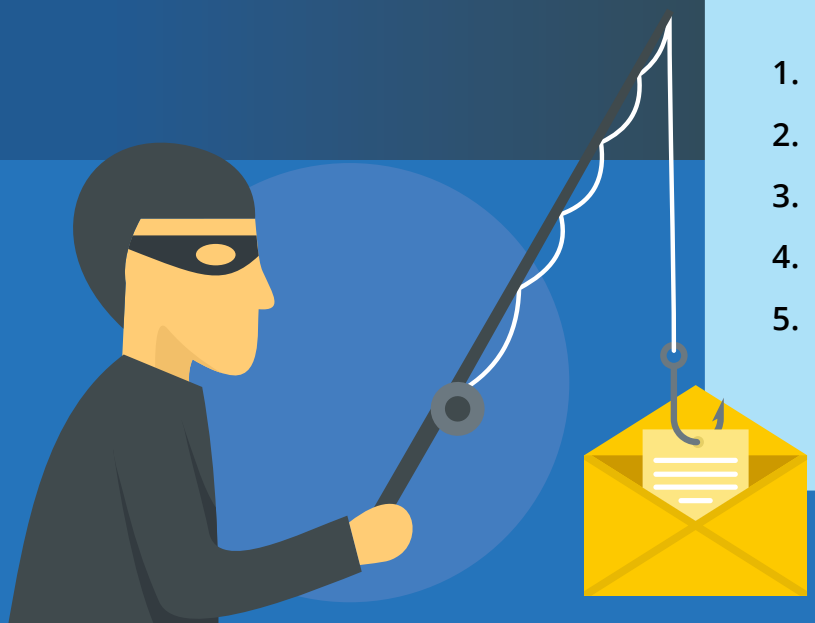
Phishing Statistics:

- The most prevalent reason for data breaches in IBM's 2022 Cost of Data Breach Report is the use of stolen or compromised credentials as a result of phishing
- In 2021, 83% of businesses said they had been victims of phishing.
- A total of 255 million phishing attacks were recorded in the first half of 2022, a significant increase over the same period the year before.

5 Tips For Avoiding Phishing Attacks

Phishing attacks are hard to spot and responsible for several cases of identity theft and data breaches. The more you educate yourself on how to protect your sensitive data, the more likely you'll be able to spot these attempts!

1. Check the sender's email address
2. Verify with the sender.
3. Check the URL of the website.
4. Check the spelling.
5. Don't open attachments from unknown sources



Password Managers continued...

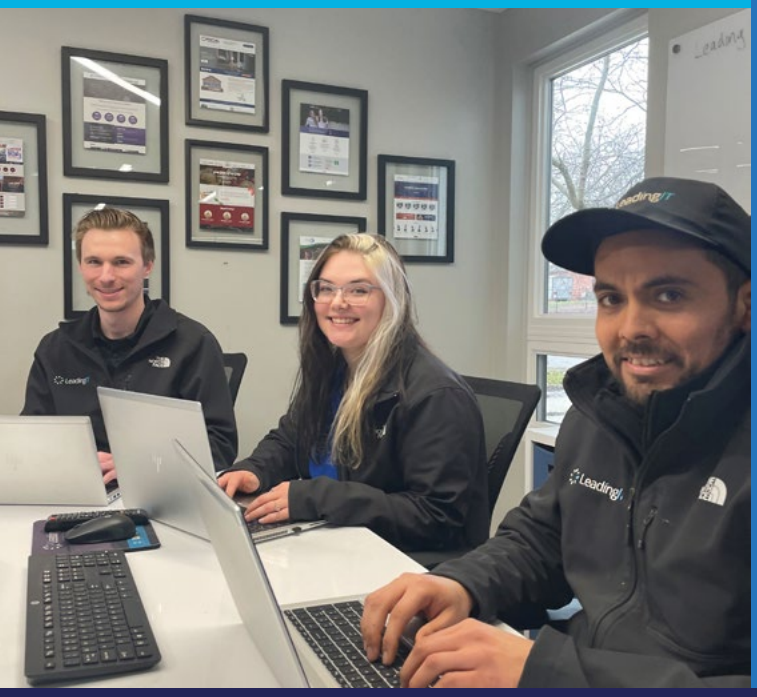
After doing so, you'll want to consider changing the passwords on your most important accounts, such as banking apps, for an additional layer of protection.

Implement Multi-Factor Authentication

Many accounts that you set up online will automatically enable multi factor authentication (MFA) that sends a verification code to your email address or phone number to ensure it's really you trying to sign in. However, some services will require you to enable MFA manually.

If you notice some of your accounts don't already use MFA, you'll want to go into your account settings to enable it.

Kyle, Mallory, Salvador



What's DLP continued...

• To track what types of files are being uploaded onto removable storage devices such as USB sticks or external hard drives - if someone tries uploading something outside their job description, then this will trigger an alert that lets you know what has happened before any damage has been done.

Why Is DLP Important?

Data protection is paramount for many companies. Sensitive data can include financial records, intellectual property, customer records, proprietary source code, and other information that must be protected from unauthorized access and leaks.

DLP helps reduce the risks of data breaches. If this sensitive information is exposed, companies can face irreversible damage, such as hefty fines and loss of consumer trust. In fact, 60% of small businesses that are breached close within six months. However, no matter the size, no company is immune to the risk of data breaches.

Protect Your Business Data

If you want to protect your company's data, a good place to start is with DLP. In this way, you can avoid costly breaches while simultaneously ensuring the integrity of your company's valuable assets.

Continue reading on our blog at goleadingit.com/blog

LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

WE ARE CELEBRATING

Birthdays

George Huebner- April 2nd
Katlyn Rogerson - April 2nd
Kyle Sandrik- April 26th
Salvador Navarro Vega - April 26th

Anniversaries

Gregory Radon - 4/19/2022