1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

December 2023

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

What's The Fuss About MFA?

Introduction

MFA, or Multi-Factor Authentication, uses multiple factors to verify a user's identity. It is typically used in addition to a username and password to provide an extra layer of security. MFA can be used for anything, from online banking to social media accounts, and can be either hardware- or software-based.

The most common forms of MFA include biometric authentication such as fingerprint scanning, facial recognition, or retinal scanning; token-based authentication such as one-time passwords sent via SMS; and knowledge-based authentication such as security questions. By using multiple factors of authentication, it makes it much harder for hackers to gain access to sensitive information.

Pros and Cons

While MFA offers many advantages over traditional authentication methods, it also has its drawbacks. The pros of MFA include increased security, better user experience, and improved compliance with regulations. It makes it harder for threat actors to crack your accounts on stolen or weak passwords alone.

On the other hand, some drawbacks include the cost associated with implementing MFA and the potential for user frustration due to having to enter

Continued on pg.2

Continued from pg.1

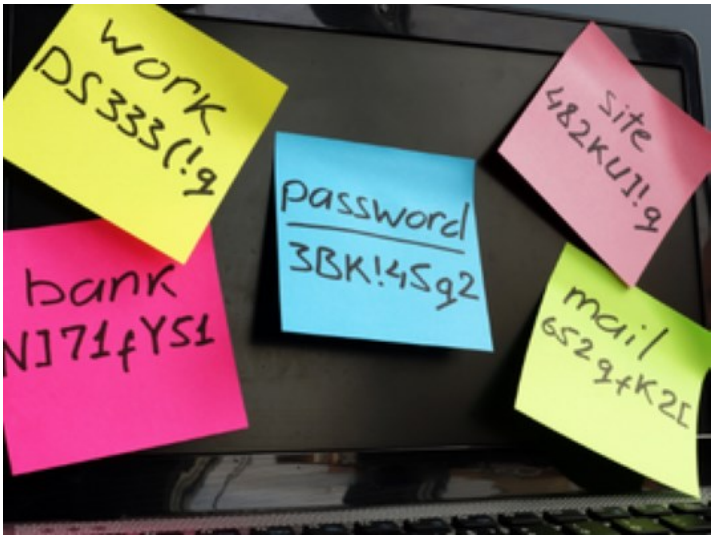
multiple credentials. It's also not impenetrable. Some ways that cybercriminals can get around MFA include:

- SIM-swapping attacks target your phone number so they can read all your texts, including one-time passwords sent via SMS
- Physical theft can lead to criminals breaking into your devices, bypassing logins completely
- Hackers can spy on devices over a shared WiFi connection and read your one-time codes
- Advanced malware can break into accounts, bypassing the MFA requirement
- SMS threads can be broken into by third parties; that's why **end-to-end encryption** is recommended for all important communications
- Exploiting your accounts after you've already logged in with MFA yourself

As you can see, there are myriad ways to exploit multi-factor authentication. Nevertheless, it's still considered the BEST way to prevent hackers from breaking into your accounts.

Conclusion

Multi-factor authentication is the best defense against brute-force attacks and hackers breaking into your accounts. While it's not *completely* impenetrable, it is the best way to keep your



accounts safe from most modern cyber-threats.

Meanwhile, that doesn't mean that you should skimp on password security! Eight characters doesn't cut it anymore. You need at least twelve letters, numbers and symbols to truly throw off determined cybercriminals and password spraying attacks. Make sure to also *never* repeat these passwords on any other account, and to change it *at least every two months.* Use a password manager to securely store complex passwords in a vault! Writing them down is dangerous.

Now I hope you understand why multi-factor authentication is so important. While not infallible, it's an extremely reliable tool for keeping out most hackers. Enable MFA to every possible account to reduce YOUR chances of a data breach

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at

https://www.cti-mi.com/itbuyersguide-1223/

NATIONAL CYBERSECURITY ALLIANCE

Stay Safe Online While Holiday Shopping!

Congratulations on making it almost all the way through 2023! Now that holiday shopping is in full swing, we wanted to let you know about a few online shopping trends we've noticed and give a few tips about how to stay safe online while buying gifts for everyone on your list.

Generally, experts seem to believe that the average American is going to spend less this year – though pandemic restrictions have largely lifted, we've entered a new season of economic uncertainty. This means every dollar is even more important, which is why we want to help you protect your hard-earned cash from the scammers and hackers that pop up every year. It's like they don't care about the naughty list! Here is what we think is cheerful and what we think is coal-worthy for shopping online this holiday season:

Merry and Bright

Keeping an eye on your bank statements

Your first line of defense against identity theft and fraud is to pay close attention to your financial records, like bank statements and credit card transactions. You can usually follow this data up-to-the-minute online. Flag any suspicious activity (like being charged for a purchase you didn't make) and contact the institution immediately.

Knowing how much items should cost

When shopping online, have a general sense of how much the items you want to buy should cost. Not only will that make you a comparison shopping extraordinaire, but you can also get a sense if an online store has prices that are too good to be true. In these cases, you might pay less, but then you might get an item that doesn't match the description, is a counterfeit, or you might pay and not get any item at all! A little bit of research can help protect you.

Making a cybersecurity list, checking it twice

This year, give yourself the gift of peace of mind by following our Core behaviors:

1. Protect each account with a unique, complex password that is at least 12 characters long – and use a password manager!
2. Use multifactor authentication (MFA) for any account that allows it.
3. Turn on automatic software updates, or install updates as soon as they are available.
4. Know how to identify phishing attempts and report phishing to your email provider or work.

NATIONAL CYBERSECURITY ALLIANCE

Stay Safe Online for Your Holiday Shopping!

Bah! Humbug!

Shopping on public wi-fi

Public wi-fi and computers are convenient, and sometimes necessary to use. However, public wi-fi is not very secure – you shouldn't ever online shop or access important accounts (like banking) while connected to public wi-fi. If you must buy a few gifts online while away from your home or work network, use a VPN (virtual private network) or mobile hotspot.

Grinch Bots

Last year, a record number of so-called "Grinch Bots" were recorded. These are automated programs that quickly buy up popular toys, sneakers, or other items and then resell the item for a huge mark-up to real people. Of course, buying supposedly new items on a resale market opens you up to an increased risk of fraud and counterfeit goods. The best way to defang Grinch Bots is to refuse to buy from them, and to only buy items from vendors you can verify.

Sharing more than you feel comfortable with

While you need to share data to make a purchase online, you should be wary of any retailer that is requesting more information than you feel comfortable sharing. Oftentimes, you don't need to fill out every field, and you shouldn't if you don't want to. If an online store requires you to share more information than you want, find another retailer on the internet – or in real life!

Keep the spirit of cybersecurity going all year long

These are some great tips for shopping safe online for the holidays, but they are also sensible habits to follow no matter what month it is. Want to make some cybersecurity resolutions for the new year? It's easy – we promise! Check out our cybersecurity basics page to learn more!

Security Corner

Falling For Common Internet Scams?

The internet is a vast and ever-changing landscape, and with that comes both good and bad. One of the downsides of the internet is the prevalence of scams.

These cyber-threats range from simple, to more targeted and complex; but there are a few recurring themes that come up in very common internet schemes which YOU will likely encounter at some point, if you haven't already.

Most Common Online Scams Around

- **Fake shopping websites** sell counterfeit products or no products at all. They often have low prices and offer free shipping to attract customers. Once you place an order, you may receive a fake product, no product at all, and your credit card information may be stolen too!
- **Fake social media accounts** may be entirely made up, or impersonate real people. The catfish behind the fake page may also send spam messages or post links to malicious websites.
- **Mobile scams** may be vishing (voice phishing, via telephone call), smishing (SMS phishing taking place over text) or other tricks to convince the target to download malware or reveal personal information.

Conclusion

Stay safe from all kinds of internet scams–and there are many!

One of the BEST safety measures that you can take is to use a strong password manager to create and manage unique passwords for all of your online accounts.

For more information about staying safe online, call us at 248-362-3800 or visit: https://tinyurl.com/3tffkamr

How To Organize Your Cybersecurity Strategy Into Left And Right Of Boom

In the pulsating digital landscape, every click and keystroke echoes through cyberspace. The battle for data security rages on. Businesses stand as both guardians and targets. Unseen adversaries covet their digital assets.

Businesses must arm themselves with a sophisticated arsenal of cybersecurity strategies. On one side, the vigilant guards of prevention (Left of Boom). On the other, the resilient bulwarks of recovery (Right of Boom).

Together, these strategies form the linchpin of a comprehensive defense. They help ensure that businesses can repel attacks. And also rise stronger from the ashes if breached.

What Do "Left of Boom" and "Right of Boom" Mean?

In the realm of cybersecurity, "Left of Boom" and "Right of Boom" are strategic terms. They delineate the proactive and reactive approaches to dealing with constant cyber threats.

"**Left of Boom**" refers to preemptive measures and preventative strategies. These are things implemented to safeguard against potential security breaches. It encompasses actions aimed at preventing cyber incidents before they even occur.

"**Right of Boom**" pertains to the post-breach recovery strategies. Companies use these strategies after a security incident has taken place. This phase involves activities like incident response planning and data backup.

Together, these terms form a comprehensive cybersecurity strategy. They cover of the equally important prevention and recovery aspects.

Left of Boom: Prevention Strategies

User Education and Awareness
One of the foundational elements of Left of Boom is employee cybersecurity education. Regular training sessions can empower staff and prevent cyber attacks.

Robust Access Control and Authentication
Access control tactics include:
- Least privilege access
- Multifactor authentication (MFA)
- Contextual access
- Single Sign-on (SSO) solutions

Regular Software Updates and Patch Management: Left of Boom strategies include ensuring all software is regularly updated.

Network Security and Firewalls: Firewalls act as the first line of defense against external threats. Install robust firewalls and intrusion detection and prevention systems and keep them updated.

Regular Security Audits and Vulnerability Assessments Conduct regular security audits and vulnerability assessments. This helps to identify potential weaknesses in your systems.

Right of Boom: Recovery Strategies

Incident Response Plan: Having a well-defined incident response plan in place is crucial. It should include things like:
- Communication protocols
- Containment procedures
- Steps for recovery
- IT contact numbers

Data Backup and Disaster Recovery: Regularly backing up data is a vital component of Right of Boom. Another critical component is having a robust disaster recovery plan.

Legal and Regulatory Compliance
Navigating the legal and regulatory landscape after a security breach is important.

Most Secure Ways To Share Passwords With Employees

Breached or stolen passwords are the bane of any organization's cybersecurity. Passwords cause over 80% of data breaches. Hackers are able to get in using stolen, weak, or reused passwords.

But passwords are a part of everyday life.

Since you can't get around passwords, how do you share them with employees safely? One solution that has gained popularity in recent years is using password managers.

Why Use a Business Password Management App?

Here are some of the reasons to consider getting a password manager for better overall data security.

• **Centralized Password Management**

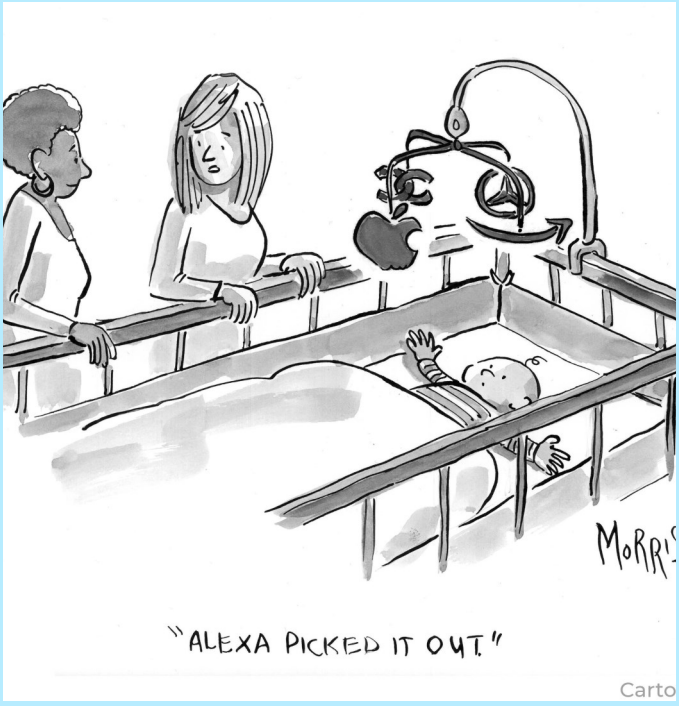
A primary advantage of password managers is their ability to centralize password management. They keep employees from using weak, repetitive passwords. And from storing them in vulnerable places.

• **Secure Password Sharing Features**

Password managers often come with secure password-sharing features. They allow administrators to share passwords with team members. And to do this without revealing the actual Password to anyone.

• **Password Generation and Complexity**

Password managers typically come with built-in password generators. They create strong, complex passwords that are difficult to crack.



9 Smart Ways For Small Businesses To Incorporate Generative AI

There is no escaping the relentless march of AI. Software companies are rapidly incorporating it into many business tools.

Leveraging Generative AI, small businesses can unlock a world of possibilities. This includes everything from enhancing customer experiences to streamlining operations. Here are some smart and practical ways to incorporate GenAI.

1. Personalized Customer Experiences
2. Presentations & Graphics Creation
3. Chatbots for Customer Support
4. Data Analysis and Insights
5. Product Design and Prototyping
6. Supply Chain Optimization
7. Dynamic Pricing Strategies
8. Human Resources and Recruitment
9. Predictive Maintenance