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

April 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!"

Avoiding Business Identity Compromise

You may have heard about Business Email Compromise (BEC) scams before. They are a type of phishing threat meant to trick you into giving up private company information by posing as a professional associate. In other words, someone pretending to be your supervisor asks for an end-of-day report. These scams have long posed a risk to organizations of all sizes. Recently, though, the FBI released a warning that cybercriminals are engaging more and more often in what's known as **Business Identity Compromise**.

Business Identity Compromise, or BIC, is a cyber-scam that steals the identifying information of a company, usually a smaller business but not exclusively, to defraud not only the organization, but also the people inside it.

Types of BIC

Over the past several years, and especially after the onset of the pandemic, these BIC scams have reached record highs according to the National Cybersecurity Society. More people working remote at least some of the time means more virtual meetings with your coworkers, which has added a new avenue for cyber-threats in many companies that weren't virtual before. So you might be a target for hackers to break into the local network; that's been true for as long as WiFi existed, and the reason to closely guard your work accounts.

However, employees can also be affected in data breaches of the company as surely as its shareholders. Not only does your employer have private data on you,

Continued on pg.2

Continued from pg.1

like your Social Security number and bank information, but they have also assigned you an employment identification number (EIN) which can be stolen too. That would equal a lot of one-on-one time with the IRS to sort out your stolen identity!

How BIC Scammers Trick You

The question thus becomes: *How* do cybercriminals launch BIC attacks, and more importantly, what can we do to protect ourselves?

Within that recent warning about the rise in BIC attacks, the FBI also noted that **deepfaking** is a common strategy for cybercriminals. This has been made possible by the advancements in AI created over the past decade, and as a result, they've made social engineering attacks even more captivating and, hence, dangerous.

Do you remember how novel it was when Facebook started *suggesting* who to tag in your photos? Since then, technology has come a remarkably long way. Now, it can generate a person's face for pictures and even include a digital recreation of their voice, on video calls. AI can now learn enough about your voice and image to recreate it. This is called deepfaking.

How does this work in real life? Say someone had the means and motive to pretend they were your boss on a video call, or a potential investor at a virtual conference. You'd be much more likely to spill the company's, and even your own, confidential information without thinking twice about it!

Protecting Yourself from Deepfakes

Avoid becoming a victim of BIC scams with many of the same tactics that you use to stave off any other social engineering attack. Deepfakes can sometimes be identified by blurry or pixelated edges around the person onscreen, as well as unusual requests or if they seem to be fishing (pun intended) for information that seems out of place.

While plenty of people keep photos of themselves online, beware how often you use your voice on camera and the security of the sites where you post those videos. An influencer with 2M Instagram followers and a daily blog would be a lot easier to deepfake than a person with their profile set to private who only accepts known friends.

Password protect your virtual meetings to ensure only those *invited* can actually join. If you get any unusual requests for money or information, even if the person appears to be speaking directly with you on video chat, it never hurts to take a few seconds to verify through the proper, secure channels that the request is genuine.

Conclusion

Cybercriminals are constantly adapting their devious ways to trick us into handing over our credentials and private information. Don't put your company's or your own data at risk! Learn how to recognize deepfakes to help protect your company and systems from Business Identity Compromise.

Do You Safeguard Your Business And Your Customers' Private Information BETTER THAN Equifax and Target Did?

If the answer is "NO" – and let's be honest, the answer *is* no – you are leaving yourself and your company open to massive liability, ***millions*** in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – social security numbers, credit card numbers, birth dates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time before they destroy your business, scare away your customers and ruin your professional and personal life.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% confidential, exclusive Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits, and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let this happen to you, your employees and your customers.

Reserve your exclusive Dark Web Scan NOW!
https://www.cti-mi.com/dark-web-monitoring-423

Security Corner

What's Up With The Phone Theft Epidemic?

Has there been a crazy rise in stolen phones in your area the past couple of years? It's not just in your head. Phone theft is more popular than ever, even in places where you wouldn't typically have been in danger of it before.

The Federal Communication Commission released an official statement, calling it an "epidemic."

If You Become a Victim

How much is a good, usable phone nowadays? Even secondhand, you're looking at a couple hundred dollars to replace your lost property if somebody swipes your cell. New ones easily run into the thousands. That's not even to mention how long you might sit in a repair store waiting to get your contacts and other data back.

To recuperate fully from the damage, half of victims pay approximately $500 to get back all their lost data. **1 in 3 people would pay one thousand dollars to get their data back.**

Physically Secure Your Devices

Take the proper steps to prevent theft from ever occurring in the first place. Keep your devices securely on your person, or better yet, leave them at home if you don't need to use them.

30M people have their phones stolen every year in the United States. Take your devices' physical security as seriously as you take online privacy!

For more information about phone theft and other cyber threats, call us at 248-362-3800 or visit: https://bit.ly/3n8m148

Data Backup Is Not Enough

The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. Most people using any type of technology have experienced data loss at least once.

There are about 140,000 hard drive crashes in the US weekly. Every five years, 20% of SMBs suffer data loss due to some type of major disaster. This has helped to drive a robust cloud backup market that continues to grow.

But one thing that's changed with data backup in the last few years is security. Simply backing up data so you don't lose it, isn't enough anymore. Backing up has morphed into data protection.

What does this mean?

It means that backups need more cybersecurity protection. They face threats such as sleeper ransomware and supply chain attacks. Cloud-based backup has the benefit of being convenient, accessible, and effective. But there is also a need for certain security considerations with an online service.

Companies need to consider data protection when planning a backup and recovery strategy. The tools used need to protect against the growing number of threats. Some of the modern threats to data backups include:

- **Data Center Outage:** The "cloud" basically means data on a server. That server is internet accessible. Those servers can crash. Data centers holding the servers can also have outages.
- **Sleeper Ransomware:** This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it's activated, the victim doesn't have a clean backup to restore from.
- **Supply Chain Attacks:** Supply chain attacks have been growing. They include attacks on cloud vendors. Those vendors suffer a cyberattack that then spreads throughout their clients.

What to Look for in a Data Protection Backup System

Just backing up data isn't enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

Ransomware Prevention

Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

95% of ransomware attacks also try to infect data backup systems.

It's important that any data backup solution you use have protection from ransomware. This type of feature restricts automated file changes that can happen to documents.

Continuous Data Protection

Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.

Threat Identification

Data protection incorporates proactive measures to protect files. Threat identification is a type of malware and virus prevention tool. It looks for malware in new and existing backups. This helps stop malware from infecting all backups.

Zero-Trust Tactics

Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multifactor authentication and application safe listing.

Why You Need To Think Twice Before Using Lensa AI & Other Self Portrait Apps

It's a common theme. You begin seeing these amazing CGI images of your friends on Facebook or Instagram and you think, "How can I make one?"

The latest of these modern vanity marvels to make the rounds is Lensa AI. You upload about 10 photos so the app can feed that data into its AI algorithm.

Then, once it maps your facial features, it generates several fantasy profile pics. It sounds like a little harmless digital fun, right?

But for Lensa AI and several similar self-portrait apps, you're paying more than you know. The cost comes from the data privacy rights you are giving up. And these can go far beyond the app itself.

Why Worry About Data Privacy with Lensa AI & Similar Apps?

Data Used to Track You
Once you download the Lensa AI app, it can track your phone activity within other apps.

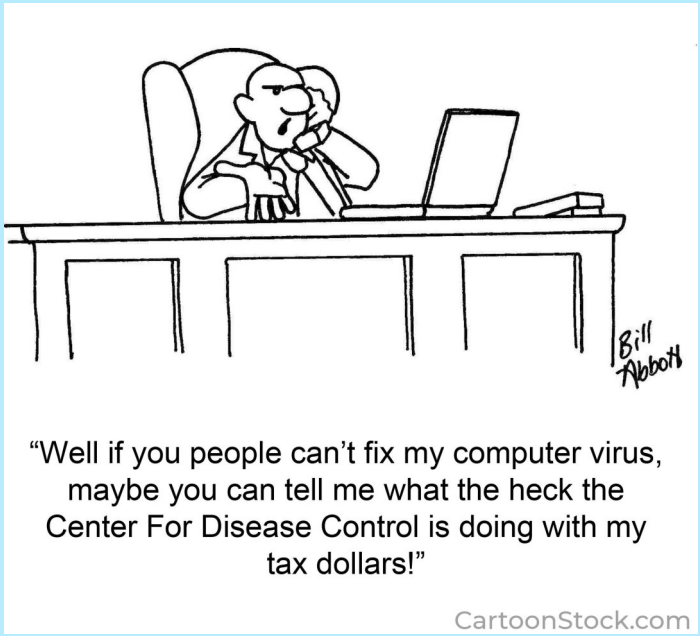
Data Collected By downloading Lensa AI, you permit it to track all kinds of data, including the purchases you make online.

Loss of Rights to Your Uploaded Images

Lensa AI Terms require you to grant a sub-licensable license to use, reproduce, modify, distribute, and create derivative works of your user content.

Get a Device Privacy Checkup

The more apps you use, the more complicated data privacy can get. Don't leave it to chance.



Every Company Is Now A Technology Company

Whether you sell shoes or run an accounting firm, you need some type of technology to operate.

Today's companies aren't just in the business of selling their own goods and services anymore.

1. Technology Is a Critical Part of Business
2. Customers Expect an Excellent Digital Experience
3. Employees Need Devices to Drive Productivity
4. AI & Automation Help Companies Stay Competitive
5. Information Is Being Generated at a Rapid Pace
7. It's Difficult to Grow Without Tech Innovation
8. Business Continuity Needs