TECHNOLOGY TIMES
INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY SINCE 2003

Defending Your College Student Against Cyber Predators

A Vital 14-Step Guide

College life today is vastly different from what it used to be. Gone are the days of shuffling from class to class with just a notebook and pencil. Nowadays, college students are armed with multiple digital devices, making them **prime targets** for cybercriminals. Surprisingly, despite considering themselves tech-savvy "digital natives," a study by Atlas VPN reveals that Gen-Z and millennials are the most susceptible to falling for phishing scams, with 20% of Gen-Zers having their identities stolen at least once, as reported by the National Cybersecurity Alliance.

Cybercriminals employ a variety of tactics to exploit this tech-savvy but vulnerable demographic:

⇒ **Unpaid Tuition Notifications**: Scammers send fake emails to students, claiming they owe money that could affect their enrollment.

⇒ **Fake Financial Aid, Grant, or Scholarship Websites**: Clicking on these sites can lead to information theft or malware installation.

⇒ **Fake Wi-Fi Accounts:** Hackers create fraudulent Wi-Fi networks in public places to steal passwords and private data.

⇒ **Social Media Scams:** Cybercriminals gather private information to hack accounts or create new ones.

⇒ **Photo and Account Blackmail:** Criminals hack phones or social media accounts to steal photos and blackmail students for payment.

These risks are compounded by several factors:

⇒ **Lack of Cybersecurity Education:** Many students aren't well

Continued on pg.2

October 2023

This monthly publication provided courtesy of David Luft, CEO of LDD Consulting, Inc.

Our Mission:

We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.

… continued from cover

-informed about cyber threats because they've relied on school or parental security.

⇒ **Over-Sharing on Social Media:** Students grew up on social media and often share personal information that can be exploited.

⇒ **Limited Credit History:** Students typically have little to no credit history, making it easier for cybercriminals to open accounts in their name.

⇒ **Multiple Connected Devices:** The proliferation of smartphones, laptops, tablets, and wearables provides numerous entry points for attackers.

⇒ **Distractions:** College life is bustling with academic and social activities, diverting attention from cybersecurity.

> **"Gen-Z and millennials are the most susceptible to falling for phishing scams, with 20% of Gen-Zers having their identities stolen at least once."**

So, what can you do? Here are 14 practical steps:

1. **Invest in Strong Security Software:** Ensure your devices have trusted virus and spyware protection, and run regular scans.
2. **Update Regularly:** Never postpone updates on your phone or computer; enable automatic updates whenever possible.
3. **Keep Software Updated:** Maintain the latest versions of browsers, extensions, and operating systems.
4. **Back Up Data:** Regularly back up your computer to the cloud to prevent data loss in case of an attack.
5. **Secure Websites Only:** Never enter credit card information on insecure websites (look for the "S" in https:// or the lock symbol.
6. **Avoid Public Wi-Fi:** Use a personal hotspot or VPN when connecting to the internet on the go.
7. **Beware of Phishing Scams:** Refrain from clicking links or opening attachments in emails, especially from unknown senders. Google websites and search for them rather than clicking links.
8. **Use Strong, Unique Passwords for every account:** Employ a password manager.
9. **Delete Cookies Regularly:** Cookies can create vulnerabilities, so clean them out periodically.
10. **Trustworthy Sources Only:** Only install software and apps from reputable sources like Apple App store or Google App store.
11. **Enable Multifactor Authentication:** Add an extra layer of security to your accounts.
12. **Password Protection:** Lock all devices and avoid sharing passwords, even with close friends.
13. **Cover Webcams:** Protect your privacy by covering webcams when not in use.
14. **Device Registration:** Register your devices with the school in case they are stolen.

Parents, make sure to go over this checklist with your college-bound children. Cybersecurity might not be their top priority, but a little effort can prevent significant consequences down the line. In today's technology-driven world, cyber threats are only going to increase.

While these tips are essential for individual cybersecurity, organizations can benefit from more in-depth cybersecurity training for employees. Seek out a professional IT service provider to bolster your defenses against evolving threats.

Free Executive Brief Reveals…
The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

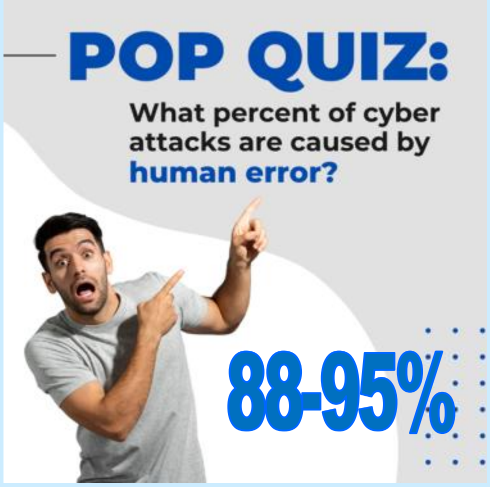
Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.

Provided By [INSERT YOUR COMPANY NAME]
Author: [INSERT YOUR NAME]
[insert your address]
[insert your web site, phone number, etc.]

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself.

Call us at 505-792-2375

to get your FREE copy today



Employee Security Training Should be a Top Priority

CREATE THE PERFECT BALANCE

Incorporating AI While Maintaining Human Connection

ChatGPT has been a hot topic in our office lately. As an author, I immediately scoffed at it. Since ChatGPT lacks emotion, it's pretty unsatisfying. Technology constantly evolves, and we must grow with it. The question is this: How do you incorporate automation and AI into your business while maintaining integral human communication?

Automating your business and utilizing AI while maintaining your integrity and humanity can be achieved through a combination of strategies. Here are five ways to accomplish it.

Identify Areas For Automation. Analyze your business processes and identify tasks that your team can automate without sacrificing the human touch. Look for repetitive, time-consuming activities you can streamline using technology.

Create System Recordings And Documents. AI can't do it all! You still need humans to help run your business. But what if someone is out, has an emergency or just wants to take a sabbatical? Here's what we do in my business: For every process, our team creates a Loom recording and a Tango document to illustrate and train other team members. This means when anyone takes a four-week vacation, nothing falls to the wayside, and there are limited disruptions in productivity (read, profitability!).

Implement AI-Powered Solutions. Leverage AI technology to automate special aspects of your business. For example, you can use chatbots or virtual assistants to handle customer inquiries, enabling human resources to respond to more complex interactions. AI can also assist in data analysis, forecasting and decision-making processes, allowing you to make informed business decisions effectively.

Personalize Customer Interactions. While automation is helpful, it's essential to maintain a personalized customer experience. Tailor your automated systems to gather relevant customer information and deliver customized recommendations or responses. This can include using AI algorithms to analyze customer behavior and preferences to provide intel on marketing campaigns.

Empower Employees. Rather than replacing humans, AI can augment their capabilities and enable them to focus on meaningful tasks. Provide training for your employees so they can work alongside AI technology effectively. This might involve developing skills in areas where humans excel, such as creativity, problem-solving and emotional intelligence. Encourage collaboration between humans and AI systems to achieve optimal results.

Remember, when it comes to automation and using AI, it's crucial to balance automation *and* humanity! By leveraging AI and personalization, your business will be able to scale and still connect with customers and clients on a human level.

Mike Michalowicz believes that he has the formula to success and has proven it on multiple occasions. He is the creator of the Profit First method*, which is used by hundreds of thousands of companies to drive profit. Mike is a former small-business columnist for The Wall Street Journal and currently leads two new multimillion-dollar ventures as he puts his latest research to the test.*

Client Spotlight

First-Class Customer Care

You will not find another IT firm here in Albuquerque with this outstanding level of customer service, period. **In our nearly four years with LDD, we have never failed to get them on the phone immediately**. The techs are professional experts in their field but still friendly and helpful regardless of how simple or severe the problem. We confidently recommend LDD! David Luft and his team will help your business run smoothly and efficiently.

Valerie Brown
Office Manager
Elite Dri-Wall
Albuquerque

Discover the Secret to Overcoming Difficult Tasks

Throughout our lives, we all encounter obstacles that appear too daunting to overcome. During these situations, most turn to the Internet or business books for advice, but there's another source everyone should turn to for support and help: someone you trust. When you partner up with someone, regardless of whether you're starting a business, tackling a project or working toward a goal, it can make the experience less stressful. Working alongside someone allows you to brainstorm ideas and find solutions you may not have been able to come up with on your own. As the saying goes, "Two heads are better than one," so find someone to help you reach your goals and start working together.

Making Technology Work for You
2420 Midtown PL NE, Suite K
Albuquerque, NM 87107

«Name»
«Company Name»
«Street Address 1» «Street Address 2»
«City», «State» «Postal Code»

Inside This Issue

The Data Breach Epidemic

How Digital Outlaws are Exploiting Human Weaknesses

Every year, thousands of businesses fall victim to data breaches. In 2022, over 1,800 data compromises affected more than 422 million people, according to the Identity Theft Resource Center's 2022 Data Breach Report. As cybercriminals continue to refine their tactics, it's clear that cyber-attacks and data breaches will not stop anytime soon. That's why it's so crucial for businesses to develop strong cyber security strategies.

If you want to bolster your cyber security efforts, a great place to start is with your employees. Research from Stanford University suggests that human error is responsible for 88% of all data breaches. In the face of relentless cyber threats, prioritizing employee training is your first line of defense against data breaches.

Online Hiring Mistakes

Many businesses have turned to the Internet for all of their hiring needs. They'll post open positions on job-board website like Indeed or ZipRecruiter, create questionnaires to prescreen potential candidates and use artificial intelligence to remove candidates with subpar resumes. Here are three hiring mistakes you should avoid:

Poor Descriptions for Job Postings: Your candidates won't be able to clarify any questions they may have about the position before applying, so your posting needs to be as detailed as possible.

Total Reliance on Automation: Automated screening processes can be a great tool during hiring, but you still need a human to ensure everything works as intended.

Failure to Inspect Resumes and Applications: Too many hiring managers avoid looking at resumes and applications until they interview candidates. Carefully review every application to craft relevant interview questions and find the best fit.