DTS DanTech Services
Computers under control!™

Technology Times August 2024 Issue

“With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you’ll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. “

What’s Inside:

Eggs, baskets, and…IT Systems

By Dan Foote

A prime example of how a well thought out plan was proven to not be so well thought out: Crowdstrike. This well-regarded cyber security service pushed out an update world-wide last week. Unfortunately, a “logic error” in the code caused Windows computers (servers, desktops, and laptops running Crowdstrike) to crash and show a BSOD (blue screen of death). Governments, enterprises, and other entities were crippled by this update.

Then there’s the time involved in restoring services because the fixed patch can only be installed to a running system. IT managers & technicians, already managing their busy schedules, just got busier to resolve this critical issue.

Word on the street is that “if you reboot your computer 15 times, it will bypass the update and boot up properly”. Not having personal experience, the thought of “fixing” a system by doing upwards of 15 reboots doesn’t thrill me at all—for a number of reasons. The webs we weave.

It becomes a rhetorical question on why a security system that integrates so deeply into an operating system would push out a global update instead of one that’s staged. Allow issues to self-identify on a level that’s manageable.

- Continued on page 3

Shiny Gadget of The Month

Ray-Ban Meta Smart Glasses

THE NEXT STEP OF SMART EYEWEAR. Ray-Ban smart glasses just got a whole lot smarter. Meta AI is a conversational assistant that you can prompt by simply saying, "Hey Meta." No need to unlock your phone or "press and hold" for assistance. With a few words, the new smart glasses can make calls, send texts, control features, and find answers for those random questions that pop into your head throughout the day.

IMPROVED AUDIO. Temple-tip speakers have higher max volume, double the bass, and better directional audio, so you can get lost in your podcast, playlist, or phone call without bothering the people around you. The five-speaker setup provides immersive audio, which renders sights and sounds through your smart glasses exactly as you would experience them in person.

ENHANCED DESIGN. Ray-Ban smart glasses prioritize lightweight comfort and durability without compromising the authentic Ray-Ban design you know and love. With two classic silhouettes and over 150 different lens and frame combinations, there's at least one option to fit every individual style.

IMPROVED CAMERA. In the outer corner of each lens is a discreet, ultra-wide 12-megapixel camera that produces bold images and videos. The improved cameras record 1080p videos of up to 60 seconds, which you can share with your contacts using AI and a quick voice command.

LIVESTREAMING CAPABILITY. Share your adventure in real time with the hands-free livestreaming feature. See community comments in your lens preview, or have AI read them aloud so you can experience the moment without interruption.

STAY POWERED ALL DAY. The redesigned smart glasses charging case offers a sleek silhouette on the outside and a powerhouse charging station on the inside. A single charge can provide up to 36 hours of use, so wherever you go, you can feel confident knowing your Ray-ban Meta glasses are up for the challenge.

Top 5 cyber threats of 2024: How to keep your small business safe

Cyber security should be top of mind for small businesses, but there's a lot to keep up with. Threat actors are continually coming up with new ways to exploit vulnerabilities in your system and get their hands on your data.

To help you prevent a data breach or cyber incident, we've researched **the top 5 cyber threats of 2024**, and what you need to know to keep your business data safe.

Ransomware remains a top – and growing – threat

Ransomware has long been a favorite money-maker for hackers and is on the rise once again. A new twist to this old crime is exfiltration ransomware, when bad actors threaten to leak data if a ransom is not paid. This variation of ransomware has the effect of feeling less dire than when your data is locked, but the result can be even costlier if data is leaked. According to the latest reports, 45% of businesses with fewer than 250 employees paid a ransom demand in order to protect confidential company data. Forty-one percent said the reason they paid was to become operational again, indicating that the security of their data is a greater concern among small business owners.

Payment diversion fraud is now the top outcome of a cyber attack

Moving up from second place, where it sat for the last two years, payment diversion fraud is now the most common outcome of a cyber-attack. PDF occurs when a hacker manipulates or deceives an employee into redirecting a legitimate payment to a fraudulent account. Email has long been used to perpetrate PDF, and now text-based attacks, known as smishing, are being added to the mix. Training employees to be vigilant and verify every email and text request for payments can help manage this risk.

Malware is harder to detect

Malware detection software has kept up fairly well with malicious software, but new methods for launching viruses and malware are starting to appear that are able to evade detection.

Bad actors are using commercial software, such as remote access and file transfer software, for malicious purposes, and the trend toward more sophisticated and elusive malware is likely to continue.

- Continued on page 4

MFA proves a critical tool for safeguarding accounts

A recent data breach at Snowflake, a Montana data warehousing company, emphasizes the importance of making Multifactor Authentication (MFA) mandatory. Cyberattackers, who were assumed to be financially motivated, targeted Snowflake's customers by testing stolen username and password pairs in the Snowflake login screen.

Although Snowflake did offer MFA, it did not require customers to use it until recently. Now, MFA will be active by default for new accounts, and existing users will receive reminders to activate it.
Not using MFA has contributed to major breaches in the past, which has made it crucial for companies to enforce it. Cloud service providers should prioritize MFA, because it is essential for protecting customer data.

Security is a joint responsibility, and both customers and providers must play their part in preventing breaches.
The recent hacking campaign against Microsoft 365 highlighted security shortcomings in licensing operations. Many plans lack essential features, such as logging capabilities, leaving data vulnerable. Customers should insist on robust identity and authentication services, urging cloud providers to enhance security. It's time for customers to use their influence and demand better security solutions from cloud service providers.

" Eggs, baskets, and ...IT system"- continued from page 1

Long ago we learned, or should have, that updates are, one, critical to protecting a system, and two, are not perfect. Microsoft knows this, as does my team. We watch for patch-related issues prior to pushing them out, which is also a reason why we patch our systems through scheduling—which isn't fail-safe either!

The complexity of systems has grown exponentially, as has the need for heightened security. Yet that eggs-baskets thing? All of them? That's troubling. It's like password reuse (don't do it!).

My prediction: smart companies will adjust their delivery systems.

*****

The many ways that technology has changed education

The rapidly changing world of technology is impacting education as much as, or even more than, it has impacted the rest of the world.

For one thing, technology has made education easily accessible for more people.   An abundance of information and trainings are available through multiple sources on the internet, and people access it throughout the world. In earlier times, only the elite had access to education, and it often required long travels to access it.

Communication and collaboration are also enhanced with the internet. In the past, classrooms were mostly isolated, and students only had access to their classmates within that room. Today, however, students in classrooms in urban cities can be taught by an explorer in a remote region, and that teaching may include videos of their experiences, interviews with natives, or a live Q&A with the explorer. The students can then share their knowledge and collaborate with other students from around the world, who are following the same lesson.

Technology also makes it easier for teachers to gather materials and prepare lessons that allow students more interaction and collaboration. But with all the information available, a teacher's role has turned into more of a guide - facilitating the students in their educational pursuits, rather than teaching the lessons directly.

Technology, and AI particularly, is opening up new possibilities for both students and faculty in their respective roles. When used as a tool and not a replacement, technology can powerfully support and transform education.

New AI technology is smaller & cheaper

To offer the power of GPT-40 to the public in a more cost-efficient way, OpenAI has introduced a new large language model (LLM), known as GPT-40 Mini.

Similar to the original GPT-40, this mini version has much of the same functionality, including a context window of 128,000 tokens (which is eight times that of GPT-3.5 Turbo). The Mini version only has text and vision support currently, but video and audio inputs and outputs are still in the works.
The Mini model includes enhanced safety features, including a greater resistance to jailbreaks (unauthorized modifications or security breaches) and improper prompt injections.

Upgrades to the Mini include a bigger context window and improvements in non-English text understanding. With these, GPT-40 Mini is ready for bigger tasks. It is ideal for processing large documents or linking multiple interactions. For example, it can enhance selection recommendations in online stores, speed up real-time customer service responses, or provide more accurate answers to students studying for exams. All these abilities will improve efficiency from previous models. Plus, it's more affordable, costing just over half the price compared to GPT-3.5 Turbo.

In terms of performance, GPT-40 Mini outshines other smaller language models like Google's Gemini Flash and Anthropic's Claude Haiku, scoring higher on Language Understanding benchmark tests. Additionally, it excels in textual comprehension, math, and coding tasks. The improved performance and affortability make advanced AI more accessible for everyday applications and ChatGPT users.

As OpenAI transitions from GPT-3.5 to more powerful models, GPT-40 Mini represents a significant step toward AGI, or Artificial General Intelligence, which is a type of AI that matches or surpasses human capabilities across a wide range of cognitive tasks. Unlike narrow AI, which is designed for specific tasks, AGI aims to exhibit human-like intelligence and adaptability.

- "Top 5 cyber threats of 2024: How to keep your small business safe" - continued from page 2

4. Artificial intelligence increases – and reduces – the risk

Artificial intelligence has been a boon for bad actors – enabling the creation of ever more sophisticated phishing emails and condensing the learning curve for malware creation. But it also aids the creation and deployment of security software and automates threat detection in email systems at networks.

5. Political cyber-attacks are on the rise

Technology is changing how military forces operate on the ground and in the air, but also online. And civilians are getting involved too. The International Committee of the Red Cross (ICRC) has issued rules for "civilian hackers" during war, effectively creating rules of engagement for hackers during wartime. These rules, while they will certainly be flouted by some, provide a basis for condemning unacceptable actions and document ethical standards for hacktivists.

Keeping your business data safe

While the methods for getting into your system can change, the steps you take to prevent intrusion stay the same. Here are some things you should be doing to protect your data.

- Educate yourself and your staff on best practices, like using strong passwords and multifactor authentication.
- Keep all your software up to date and patch as required.
- Back up data regularly.

Secure adequate and appropriate cyber security insurance for your business.