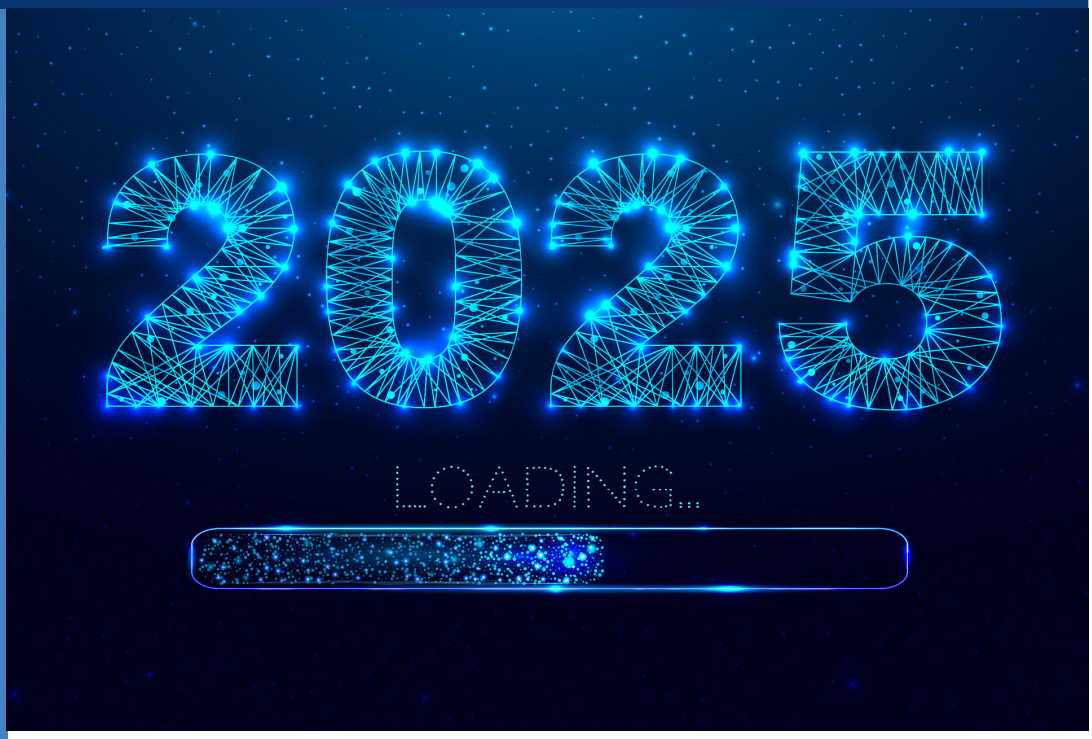
DTS DanTech Services
Computers under control!™

Technology Times January 2025 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:



The Future of Cybersecurity: Key Trends for 2025

As we approach 2025, the rapid evolution of the digital landscape presents new cybersecurity challenges for businesses worldwide. Advanced AI technologies and an integrated approach will be crucial for effective network security. Here are eight major trends expected to redefine cybersecurity strategies:

1. Secure Browsers Become Essential

With the shift to browser-based work and remote access, secure browsers will be critical in preventing data breaches and ensuring safe access to digital tools, regardless of location or device.

2. Government Investments in Smart Infrastructure

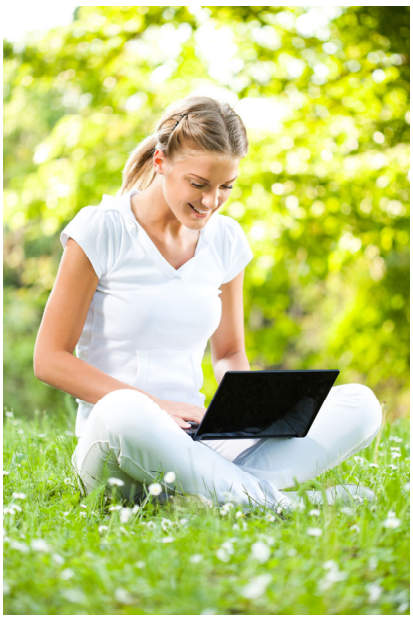
In response to increasing nation-state attacks, governments will enhance their infrastructure security by investing in modern technology and prioritizing 5G to support smart cities, addressing vulnerabilities in critical systems.

3. Post-Quantum Cryptography (PQC) Attacks

The rise of PQC will allow attackers to exploit security weaknesses in systems that aren't updated to handle encrypted traffic. Organizations must ensure their security measures can decrypt and inspect this traffic.

- Continued on page 3

Digital Diet: A Tool to Improve Mental Health With Positive Browsing



Researchers at MIT have found that people struggling with mental health issues are more likely to browse negative content online, which serves to exacerbate their symptoms. The study analyzed the web browsing habits of more than 1,000 participants and used natural language processing to score the emotional content of web sites. The findings revealed a mutual impact between mental health and online behavior, where negative content worsens mental health symptoms, creating a feedback loop.

The researchers developed a web plug-in tool called "Digital Diet," to help users make better decisions about the content they view. The tool gives scores for pages based on their emotional impact, knowledge value, and actionability. Participants who used the tool were less likely to choose negative content and reported improved moods after browsing more positive content. The researchers hope to break the cycle of negative content viewing and improve mental health outcomes.

These study results contribute to the ongoing debate about the relationship between mental health and online behavior, emphasizing the importance of the type of content consumed rather than just the quantity. Using tools like Digital Diet, researchers hope to empower individuals to take control of their online experiences and protect their mental health.

Indictment of 14 North Korean Cyber Criminals Points to Increasing Need of Cyber Vigilance

North Korean Nationals involved in a scheme to defraud US companies were indicted by a federal court in St Louis, Missouri, on Dec. 11. Fourteen North Koreans posed as IT workers -- using false identities to secure remote jobs -- and funneled their earnings, which totaled more than $88 million, back to North Korea.

The scheme, orchestrated by two North Korean-controlled companies, Yanbian Silverstar and Volasys Silverstar, took place over approximately six years, and involved stealing sensitive information from companies and extorting them by threatening to leak this data.

The charges against each of the 14 conspirators include conspiring to violate the International Emergency Economic Powers Act, and conspiracy to commit wire fraud, money laundering and identity theft. Eight of the 14 are charged with aggravated identity theft. If they are convicted, they each face a maximum statutory penalty of 27 years in prison.

The indictment is part of a broader National Security Division Initiative to disrupt North Korean cyber activities. The US has taken other legal actions toward this cause, including the seizure of $2.5 million and 29 internet domains used in the scheme. The State Department is offering up to $5 million for information leading to the disruption of these illicit activities. The FBI and cybersecurity officials say they will continue working toward securing American businesses against fraudulent IT schemes, and they vow continued support to victims of international cybercrime.

Since North Korea's IT workers pose a sophisticated and persistent threat, businesses must remain vigilant. Authorities have issued advisories to help companies recognize and mitigate such threats, emphasizing the need for thoroughly vetting remote IT workers before hiring. Promote a culture of vigilance by following these tips:

- Incorporate regular employee education and cyber training to help employees and management recognize and respond properly to suspicious activities.
- Implement Multi-Factor Authentication (MFA) for accessing company systems and sensitive data to add an extra layer of security beyond passwords.
- Adopt a zero-trust security model where every access request is verified, regardless of whether it comes from inside or outside the network.
- Perform regular security audits and penetration testing to identify and address vulnerabilities in your system.

- Continued on page 4

US to Take the Offensive Against Cyber Terrorism

The new cabinet is making plans to impose steeper penalties on cyber criminals targeting the US, according to Rep. Mike Waltz, the incoming national security adviser, in a speech he made in Milwaukee on December 15th.

This statement follows a massive Chinese cyber espionage campaign, known as "Salt Typhoon," that recorded phone calls of American political figures and stole large amounts of data. At least eight telecommunications and infrastructure firms have been affected. Chinese officials have dismissed the allegations as disinformation, stating that Beijing "firmly opposes and combats cyber attacks and cyber theft in all forms."

Waltz believes Washington has focused for too long on its cyber defenses and now needs to go on the offensive by imposing higher costs and consequences to cybercriminals, individual and state sponsored, who steal data and spy on the US.

"This is wholly unacceptable, and I think we need to take a much stronger stance," Waltz said, noting that the US tech industry can help make adversaries vulnerable and aid in US defense.

Big tech firms that handle all the data streams entering and exiting US networks should scrutinize international data traffic more closely.

Smaller companies and individuals also play a big role in the cybersecurity of this nation by following the standard protocols, such as keeping anti-virus software and browsers updated and using strong passwords. These are our best defenses against cyber attacks.

"The Future of Cybersecurity: Key Trends for 2025" - continued from page 1

4. Multivector Attack Strategies

Cybercriminals will use a combination of tactics across multiple vectors for more sophisticated attacks. Organizations will need integrated security services to effectively defend against these complex threats.

5. AI Addresses the Skills Gap

As demand for cybersecurity professionals continues to grow, AI-powered tools will assist in automating tasks and providing insights, helping fill the skills gap and enhancing security operations.

6. Adoption of Single Vendor SASE Solutions

With the increase in remote work, organizations will widely adopt single-vendor Secure Access Service Edge (SASE) solutions to ensure secure, high-performance access to critical applications.

7. Rise in AI-Specific Attacks

As organizations adopt AI technologies, vulnerabilities will emerge, leading to an increase in targeted attacks. Comprehensive, AI-driven security solutions will be necessary to safeguard sensitive data.

8. Advanced Phishing Techniques

Generative AI will enhance phishing attacks, making them harder to detect. Companies will need robust AI-powered security measures, including secure browsers and integrated SASE solutions, to combat these threats.

Preparing for 2025

Organizations must prepare for the future of network security by adopting agile, holistic strategies that utilize new technologies such as secure browsers, AI tools, and SASE solutions. By doing so, they will not only protect against current threats but also ensure resilience in the face of evolving cyber risks. As we move toward 2025, a proactive approach will be essential for safeguarding valuable assets in a dynamic digital environment.

Ryoko Has it All

Today, Ryoko has reached a new level of excellence. It's packed with all the features you've come to need and love, and more!

How Does It Work?

Ryoko automatically **connects to the closest internet tower in 76 countries**. By working with leading global internet providers, Ryoko ensures a consistently reliable, fast, and secure internet connection for all your devices, no matter where you are in the world.

Connect 10 Devices

From phones to laptops, tablets, and beyond. Share the connection with friends and family too!

Fits in Your Pocket

Enjoy the freedom of internet on-the-go. Ryoko operates wire-free, is lightweight and portable!

Fast-Charge with USB-C

Charges fast, with any USB-C cable. For your convenience, you'll find one in the package together with Ryoko

Data Saver

Get high-speed Internet with data efficiency optimization.

Long-Lasting Battery

Up to 8 hours of WiFi life keeps you connected without interruptions.

Fast Internet Connection

Experience a high-speed connection of up to 150MB/s. Supports multiple devices easily.

Simple to Use

With a user-friendly design, Ryoko is easy to use for people of all ages.

- "Indictment of 14 North Korean Cyber Criminals " - continued from page 2

- Limit access to company systems based on IP addresses to ensure that only authorized locations can connect.
- Continuously monitor network activities and maintain logs to detect and respond to unusual or unauthorized actions promptly.
- Ensure remote workers use secure connections, such as VPNs, and avoid public Wi-Fi for accessing company resources.
- Implement strong identification processes during hiring and for accessing sensitive information, possibly including background checks and biometric verification.
- Promote a culture where employees feel comfortable reporting any suspicious activities or potential security breaches without fear of repercussions.

An intricate vetting process is of utmost importance when hiring for critical positions that deal with sensitive data!

Want to Avoid Lost Luggage? Add an AirTag.

Apple's AirTags, which rely on the vast network of millions of Apple devices, have made the news for helping users track down stolen items and even finding loved ones suffering from dementia. So it stands to reason they could easily help you locate lost airline luggage.

Here are some tips for keeping tabs on your bags with AirTags.

Be Strategic About the AirTag's Placement: Keep it on the inside of the luggage, placed against a side rather than mixed in with your belongings to ensure it doesn't get snagged, snatched by a thief, or blocked from transmitting its signals.

Keep Your Apple Devices Updated: Make sure all your Apple devices are running updated software. Certain features that are AirTag related, including anti-stalking alerts, require iOS 17.5 or later.

Use Lost Mode: Go to Items >Find My App and click on the name you assigned the AirTag to see its current or last seen location. The Lost Mode, also helps you keep a close eye on your bag, alerting you when it moves to a new location.

Share Item Location: If your luggage is missing, you can share the AirTag with participating airlines by selecting Share Item Location to bring up a webpage showing the tracker's location. Then copy and paste the link into your airline's delayed-bag claim portal.

Make Sure Battery is Full: Apple batteries last about a year. You can track the phone's battery status by clicking the Find My app. A red battery icon indicates that the battery needs to be replaced.

Other Trackers Work, Too: Pebblebees Clip, Chipolo Card Spot and Apple's Precision Finding, are tracker options that also work well.

Don't Just Rely on the Airtag: Be responsible by arriving an hour ahead of time, making your bags easily identifiable, and putting your contact info (name, email, and phone) on a luggage tag to prevent other customers from taking the wrong suitcase.

The AirTag trackers appear on the Find My app's map alongside other Apple gadgets. Google offers a similar network, and Android users must opt in to participate.