DTS DanTech Services
Computers under control!™

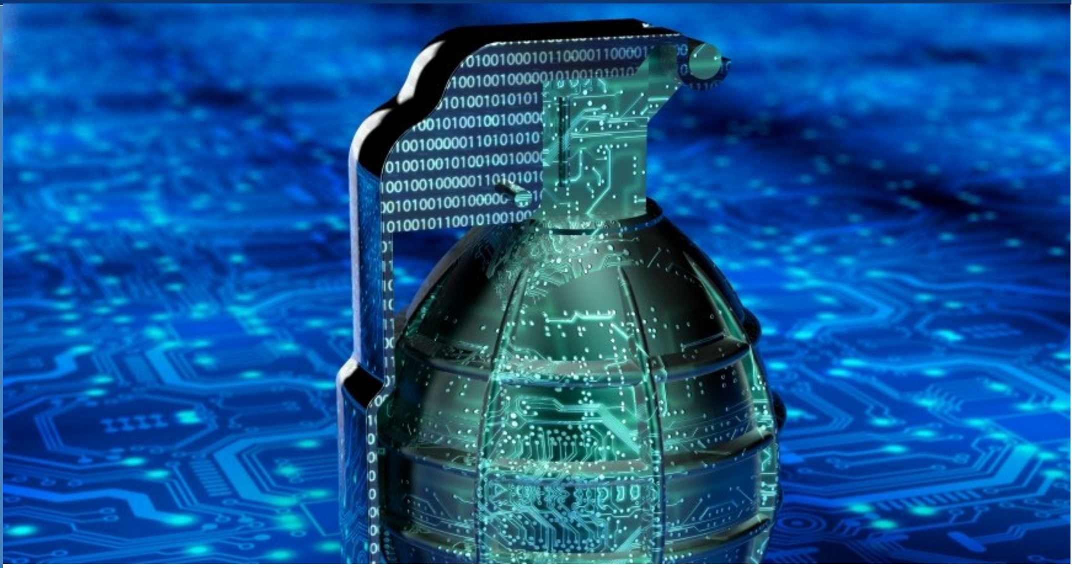
Technology Times April 2022 Issue

"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. "

Dan Foote
Owner/President

What's Inside:

Got IT Problem? - Click Here!



A cyber attack may hit the US — how to protect your data and devices

As Russia deploys brute force to invade Ukraine, the US fears that the nation may have another tactic up its sleeves: cyber warfare. Last week, President Joe Biden warned business leaders about the looming threat of cyber attacks that could cripple US infrastructure.

You may be wondering, "What does cyberwarfare look like and how can it affect me?" Let's take a look at what the experts have to say so that you can keep your data and devices protected in the event of a cyber attack.

What would a Russian cyber attack on the US look like?

In a written statement, the Biden Administration issued a warning that the Russian government may knock the US off its feet using cyber attacks. Biden added that cyber warfare is a "part of Russia's playbook."

In other words, Russia is no stranger to using hacking strategies to undermine its enemies, which gives us a glimpse of how cyber warfare could play out if the invasive nation decides to attack the US' technological vulnerabilities. Here are some cyber attacks in recent times that paint a small-scale picture of warfare in the cyberworld:

- **A pair of cyberattacks, widely established as Russian-linked hacking, hit some parts of Ukraine after Russia's annexation of Crimea eight years ago.** In 2015 and 2016, hackers managed to take out power in some parts of Ukraine, according to Vox.

- Continued on page 4

Mobile Cybersecurity Trends

Mobiles have become an extension of our arms. We use them for anything, and everything — from checking our heart rate to making sure a photo frame hangs straight. Over six billion people worldwide use smartphones, including 85% of Americans. In the U.S., mobile e-commerce spending topped $47 billion. We see fraud trends that businesses need to be on the lookout for this year:

Mobile app fraud. Lots of it. Period. It's easy to defraud an app especially given the low barriers to entry. In 2020, a massive fraud operation used a network of devices to drain millions from online bank accounts at record speed. A single emulator spoofed over 8,000 devices. These malicious tools are so readily available we expect to see many more instances this year. To combat it, mobile apps need to dial up their anti-fraud efforts. If they don't, they run the risk of being defrauded across every service they offer.

Cross-border fraud. Cross-border e-commerce transactions spiked to obscene levels in 2021, with consumers under lockdown. But where there is smoke, there is usually fire. Spikes in sales led to spikes in fraud. In 2021, more than 60% of U.S. and U.K. businesses reported issues with cross-border fraud, and global card not present fraud tripled to over $32 billion in the last few years. As travel start to recover, fraudsters will take advantage of travel-starved individuals. Fake accounts, websites, and apps to trick people into purchasing travel packages that don't exist will start to pop up. In addition, two years of travel restrictions have left some travel accounts dormant, and it's been easier for fraudsters to break into them and drain loyalty points or stored value. Businesses need to pay close attention to new patterns of activity and secure their platforms.

Account Take Overs (ATO). Battling ATOs is a never-ending game of whack-a-mole. Years of massive data breaches have made it easy for fraudsters to acquire user credentials. Data leaks continue to be on the rise. Breaches in 2021 surpassed those in 2020 by almost 20%. As a result, ATO attempts will start to surge even higher in the coming months. It's not just the number of accounts being breached; it's how. Advances in deepfake technology have led to more effective social engineering scams. Cybercriminals are also using A.I. and machine learning to engineer attacks. They are often bad bots as they mimic actual user login behavior and attempt thousands of user login attempts in seconds.

Reports: Russian IPs Scanning US Energy Firms, Others

Bulletin Reportedly Issued Just Days Before Biden Warned of Cyber Activity

Just days before U.S. President Joe Biden warned that intelligence is pointing toward potential Russian cyberattacks against the U.S., the FBI reportedly issued an urgent bulletin contending that Russian IP addresses have conducted network scanning activity on at least five U.S. energy firms.

According to CBS News, which first broke the news, the activity has been pegged to threat actors who "previously conducted destructive cyber activity against foreign critical infrastructure." Now, the bureau is reportedly saying that the activity of the cited Russian IP addresses likely amounts to network reconnaissance to identify vulnerabilities to enable (potential) future intrusions. The FBI has cited 140 IP addresses it says connect to "abnormal scanning" activity toward the aforementioned U.S. firms, CBS News reports. Some 18 other U.S. companies across the defense industrial base, financial services and information technology were also reportedly targeted. According to the same report, the bureau detected the anomalous activity beginning March 2021.

FBI officials also reportedly are seeing an uptick in scanning since Feb. 24, the start of Russia's invasion of Ukraine. Officials reportedly say the IPs have been "previously identified" actively exploiting foreign victims, leading to the "destruction" of their systems. The FBI has also provided indicators of compromise - though the addresses, at this time, cannot be directly tied to successful exploitation, officials say.

'Call Us If You See Something Suspicious'

In a statement on Tuesday, the FBI said: "The FBI, along with our federal partners, remains committed to investigating and combating any malicious cyber activity targeting the U.S. The FBI has consistently disseminated public threat advisories warning about these activities conducted by Russian cyber actors. We continue to share information proactively with our private sector partners to identify targeting and prevent incidents. We encourage the public to report any suspicious cyber activity to www.ic3.gov."

FBI officials urge those in the public sector to use strong passwords and multifactor authentication and to perform patching and regular software updates. The bureau encourages network defenders in the private sector to review recent cybersecurity advisories and continually review alerts from the Cybersecurity and Infrastructure Security Agency. "Know if your company has any connectivity in Russia and surrounding territories," the bureau states. "Exercise cybersecurity incident response plans, and, if compromised, the FBI encourages reporting information promptly to the local FBI field office."

Earlier this month, the U.S. Congress passed an omnibus spending bill that carries a mandatory cyber incident reporting provision for critical infrastructure providers - within 72 hours - and reporting within 24 hours after any ransom payment is made (see: *US Congress Passes Cyber Incident Reporting Mandate*). Commenting on the FBI's bulletin, Rajiv Pimplaskar, CEO of the security firm Dispersive Holdings Inc., tells ISMG: "Nation-states have virtually unlimited compute and people resources at their disposal, and their toolkits can be highly effective against industry standard(s). … Nation-state toolkits can use public cloud as a gateway to get underneath the encryption layer and capture the data flow itself for future analysis." Pimplaskar adds: "Critical infrastructure companies should bolster their cyber defense posture with advanced communications security that can obfuscate resources, as well as leverage data multi-pathing to present a harder target for such threat actors."

Shiny New Gadget Of The Month:

KardiaMobile EKG Monitor - Instant EKG on Your Smartphone

FDA-cleared personal EKG: The world's most clinically validated personal EKG, FDA-cleared to detect Atrial Fibrillation, Bradycardia, and Tachycardia. KardiaMobile is the most reliable way to check in on your heart from home.

- **Take your EKG from anywhere**: Capture a medical-grade EKG in 30 seconds and get an instant analysis right on your smartphone. KardiaMobile is small enough to fit in your pocket, so you can take it with you anywhere.
- **Easy to use**: Simply place your fingers on the sensors—no wires, patches, or gels.
- **Recommended by doctors**: A trusted resource, KardiaMobile is the #1 doctor-recommended personal EKG with more than 100 million EKGs recorded.
- **Save or share your EKGs**: With the press of a button, email your EKGs to your doctor or save them on your phone.
- **Works with smartphones**: Compatible with most Android and iOS smartphones and tablets.
- **FSA/HSA eligible**: Purchase using an FSA or HSA account (please confirm coverage with your insurance provider).

Phone clip included with purchase: a $15 value. Conveniently take your device with you wherever you go.

Note: KardiaMobile is not recommended for use with a Pacemaker

Transitioning to Windows 11

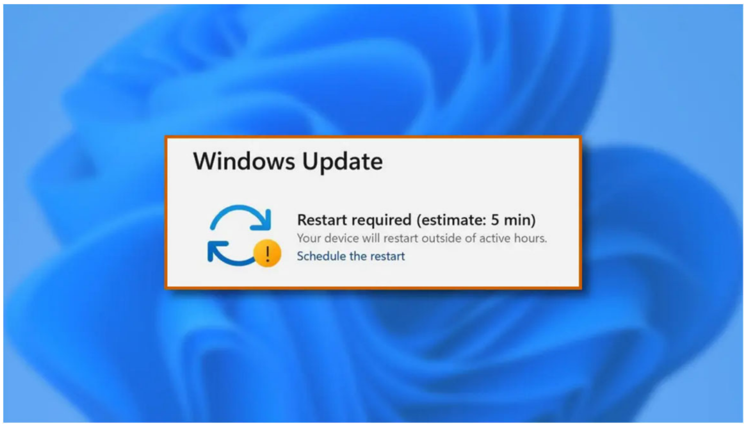
OS developers are always looking for approval—even if it's forced approval via numbers of users. Windows is sneaky that way. "Here's a security update." – and it turns out to be an OS upgrade. Gee. Thanks.

While we attempt to block the Windows 11 upgrades through our management system, home users won't be as fortunate and, one day, will possibly see a longer load time with a different appearance once it has finally loaded. Gee. Thanks.

This is where some confusion can become apparent. The Taskbar is in a fixed position—and cannot be moved. Taskbar drag-n-drop functionality fails, and other functions have been removed. Program buttons are grouped (combined), don't show text labels, and your forced into the "we've made decisions for you" path by removing the ability to resize the Taskbar. Gee. Thanks.

Fortunately, there are fixes to restore many of the functions that we've become accustomed to. Unfortunately, many of them require registry tweaks, which requires the ability to follow exact instructions because making improper registry changes can break your computer.

There are programmers that have scripted these changes into quickly applied patches, yet it's very important that any scripts used for these purposes are valid and not malicious—which brings us to an entirely different level: how do you know? Trust of the developer is key, yet if you don't know whether the scripter can be trusted, then a review of the script is necessary to make sure it doesn't inject malware or break your computer.



Windows Update

Restart required (estimate: 5 min)

Your device will restart outside of active hours.

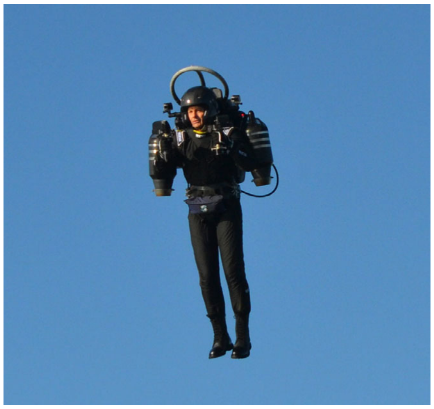
Schedule the restart

At DanTech Services, we have yet to allow wide-spread release of Windows 11 updates as our comfort level has yet to be satisfied. OS Updates have been known to break other functionality, the issues noted above, and making sure we can adequately support it are key, yet all in all, Windows 11 just needs to be a bit better from a usability perspective. That, and stability. Plus, there are certain hardware requirements that must be met, which means that older machines will never see a Windows 11 upgrade.

BTW, there's a small window of time after a Windows 11 upgrade where you can revert back to Windows 10. Please let us know if you need assistance in a downgrade or other Windows 11 issue. Oh, and back up your data!

Dan

Suit Up!



Just three years ago, British inventor Richard Browning broke his own speed record by flying his jetpack invention nearly 100 miles per hour. That's no typo — according to a *Daily Mail* article published in 2019 and shared by his company Gravity Industries, the aptly-nicknamed "Iron Man" Browning more than doubled his previous record of 32 mph by hitting a blistering 85 mph with his rig.

That high speed is surely part of what made the Jet Suit attractive to the UK's Lake District, which is set to equip paramedics with their own Jet Suits for emergency response.

According to a *BBC* report published days before, one member of Great North Air Ambulance (GNAA) staff has completed training to use the suit solo, and two more will start soon.

"We're still awestruck by it, everyone looks at the wow factor and the fact we are the world's first jet suit paramedics but for us it's about delivering patient care," Andy Mawson, GNAA operations director who's completed the training, told the UK news outlet. The idea is to get paramedics to patients in need of emergency care faster than ever, which could mean more people survive than if they experienced a longer response time.

Gravity Industries isn't the only company creating jet packs for emergency or government use cases. David Mayman of JetPack Aviation has already sold two units to an undisclosed military client in South Asia, and says the future of medical and emergency response could very well be aloft his own super-fast Speeders, which look sort of like flying motorcycles.

"Russian cyber attack possible"
Continued from Page 1

- **In 2017, Kremlin-backed malicious actors unleashed a vicious ransomware attack in Ukraine.** Dubbed NotPetya, this malware wreaks havoc by encrypting victims' data and locking them out of their own files. Victims had to pay a ransom of $300 in Bitcoin to retrieve their files. NotPetya was so poisonous it spread beyond Ukraine's borders. According to Vox, it's one of the worst cyber attacks in modern history.
- **Last year, the US fell victim to a cyber-attack known as the Colonial Pipeline Hack**. In May 2021, a group of Russian-linked hackers called DarkSide breached Colonial Pipeline Co. (a major oil pipeline that carries petrol and jet fuel to the US' southeastern region). Hackers held the company's data for ransom, disrupting the pipeline's flow. Colonial was forced to pay nearly $5 million to restore its data and network.
- **Most recently, Ukraine was the target of distributed denial of service (DDoS) attacks in late February**, which was deployed shortly after the Russian invasion. According to CNBC, several Ukrainian government websites were offline as a result of the attack.

Looking at the precedent for Russian cyberattacks, fuel pipelines, power grids, major computer networks and more are in jeopardy. To add insult to injury, cyber warfare could spill over into US banks, affecting Americans' hard-earned money. Don't worry, though. We have some tips on how to protect yourself if hackers wreak havoc in US' cyberspace.

How to protect yourself from potential cyber attacks

Last week, the White House rolled out a fact sheet urging businesses to tighten their security practices. Although the fact sheet targets major companies, there's an abundance of useful information anyone can use to shield their data, devices and digital assets from cyber-attacks.

1. **Use multi-factor authentication.** Additional layers of security hinder hackers from infiltrating your system
2. **Deploy anti-malware security tools on your computers and devices frequently.** This ensures that you're continuously on the lookout for threats. Check out the best anti-virus software apps on the market.
3. **Consult a cybersecurity professional to ensure you're protected against vulnerabilities.** Often, it's best to ask an expert.
4. **Switch passwords regularly.** In this way, stolen passwords are rendered useless to hackers.
5. **Back up your data in the event of a breach.** Make sure this backup is stored offline out of hackers' reach.

QUESTIONS?