DTS DanTech Services
Computers under control!™

Technology Times February 2021 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:

Got IT Problem? - Click Here!

"If we've learned anything about cyberattacks in 2020, it's that nothing is off-limits and everything is fair game."

2020, of course, was no ordinary year, and a spike in cybercrime that sought to exploit a crisis and disrupt recovery efforts truly tarred the blackhat industry as one where nothing is off-limits and everything is fair game.

Amid the strain of a global pandemic, continued **attacks on hospitals** and healthcare facilities took place, ransomware targeted the stalling education sector – including universities and high schools – and an attack was even detected targeting the **cold supply chain of vaccination** efforts.

For most businesses, the move to remote working brought heightened risk, with familiar on-premise IT networks exchanged for home wi-fi and personal devices.

As we roll toward a new year, independent cybersecurity and data privacy consultancy Bridewell Consulting issued six predictions that will impact cybersecurity in 2021.

 # 1 | Sustained remote working provides new challenges As a result of the Covid-19 crisis, increased home and remote working, decentralized workforces, and outsourcing of skillsets are all contributing to a huge increase in connected devices. This in turn increases the number of risks associated with centralized data and infrastructures, as well as vulnerabilities around multiple access points.

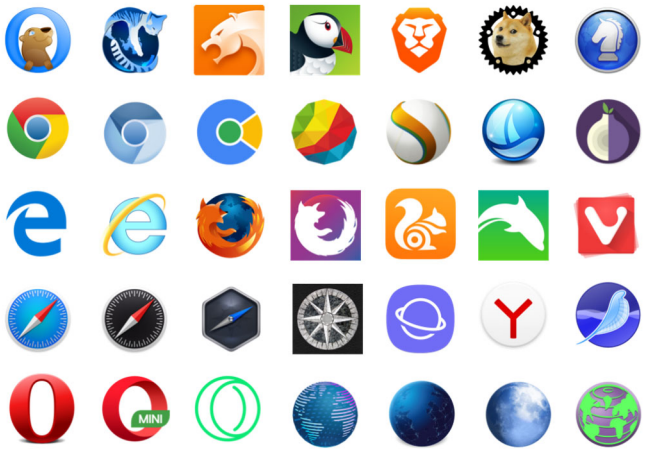
- Continued on page 3

Go to the Internet

By Dan Foote

"Go to the Internet" is usually a phrase that gets a funneled translation of, "Oh, I need to do this and find that." The This and That are translated into open a web browser and search for the website I want to go to. Let's talk about the "This" in our statement: Open a Web Browser.

There are a number of web browsers used today. A short list of the most popular contains: Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari, Opera, and the now deprecated Internet Explorer. This doesn't even begin to list the dozens of other variants that are out there that you've likely never heard of, so we will stay with the more popular (for more of everything, here's a list of 120 browsers!).



The choice of web browser that you use can largely be a personal one. "I'm comfortable with _____" –which is important! It's good to be comfortable with your tools of choice, yet will your preferred browser work for you in all instances or provide the level of speed, security, or privacy you require? My broad, brush strokes on this issue are as follows:

Speed:

By all indications, the Chromium-based Microsoft Edge browser gets the best speed results. This is the _*new*_ Edge browser, which I find to have far better function and capabilities than its predecessor. Firefox also gets high marks in speed, as does Opera.

Security:

Of the popular browsers, Firefox has the best security, which also translates to privacy, in my opinion. If you're looking for a Chrome-alternative that provides a higher level of security than Chrome, try Brave. It too is chromium-based.

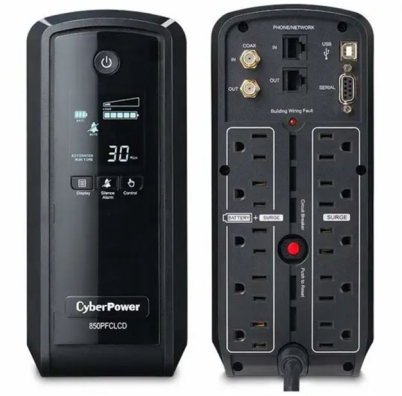
Privacy:

Browser privacy (and security) are dictated more by the users' actions than anything else. What extensions or add-ons are installed? These "options" can create security & privacy holes that compromise you and your data. BTW, the use of Private or Incognito browser windows do little to protect either your privacy or security, yet they do have an excellent purpose of providing a shield for how cookies, browser history, and web caching can affect site access.

On your computer(s), in addition to the default browser installed by the operating system, I recommend that you download and install both Firefox & Google Chrome. You may even know why as there are websites that will only work in Chrome, which has become the de-facto browser of many users. My personal browser of choice, currently, is Firefox and it's set up with Duck Duck Go as its default search engine. You may glean from this that I want speed, security, and privacy as my Go To—and you'd be correct. I can do 90% of my work in Firefox with this combination. And I can switch as needed by using a different browser or search engine.

While a "web browser is a web browser" has some truth to it, the differences can be important—at least they are to me. Yet do not fear the browser. Try out the different browsers on the same sites. See what works best for you—and beware those extensions!

Shiny New Gadget Of The Month:



CyberPower CP850PFCLCD PFC Sinewave UPS System

A **mini tower with 10 outlets** that'll act as a battery backup so (God forbid!) the power goes out, you won't lose all the progress you made building your dream home on *The Sims*.

Promising review: "I am the proud owner of three of these (so far). They're quiet when on AC power. They have great customization. I've muted the beeps and warnings so if the power kicks off, they just take over without distracting me further. I LOVE the two front USB plugs. I charge devices from them all the time. The LED screen is off by default until you press a button, so other than the dimly lit power button on the front, there's no distracting lights or sounds under normal use on AC power.

So, how well do they work? Well, I've owned a lot of UPSes. These are by far much quieter than any I've purchased from APC. They have a true sine wave output (which is amazing!), and the 1500VA is perfect for most electronics. The front screen will tell you how much of a load you have plugged in and even an estimate for how long the unit should run given that load if you lost power. So, no surprises!"

"Six cybersecurity trends heading our way in 2021"
- Continued from Page 1

In 2021, cybersecurity will be even more difficult to ensure as the attack surface is bigger and the measures to implement and control security and data policies are often lacking in a remote environment.

 # 2 | Death by cyber-attack A major concern is that we may start to see the first deaths associated with a cyberattack, as hospitals are stretched and attackers are continuing to target healthcare. The sector is particularly at risk due to the massive economic and operational impacts it is currently suffering – sadly we have already seen such a case in Germany. A homicide investigation was launched after a patient died in a Düsseldorf hospital that had its systems knocked by a cyber-attack. If this leads to a prosecution, it would be the first confirmed case in which anyone has died as the direct consequence of a cyber attack.

 # 3 | The evolving threat Another impact of remote working will be more organizations relying on IoT devices for measuring and monitoring processes. With the continued expansion of IoT, along with the rollout of 5G, cyber attackers will be relishing the growing opportunity to compromise systems and networks, as even more devices become connected to the internet. Organizations still need to adequately segregate insecure IoT and 5G-enabled devices from the rest of their network. In healthcare, for example, wearable IoT sensors enable remote patient monitoring, so unsecure devices could facilitate the misuse of sensitive patient data. .

 # 4 | Detection, not just protection Despite these new threats, there are hopeful signs that the sophistication of defensive security will finally catch-up with its offensive counterparts due to new innovation and capabilities. Technical cyber-defense will still be of uppermost importance, along with the need to focus on detection of cyber-threats, not purely protection and prevention. Over the next year, there is likely to be an acceleration in the use of Cloud SIEM (Security Information and Event Management), with human-guided threat hunting, supported by machine learning-powered SIEM tools like Azure Sentinel, helping to uncover infiltrators before they access sensitive data.

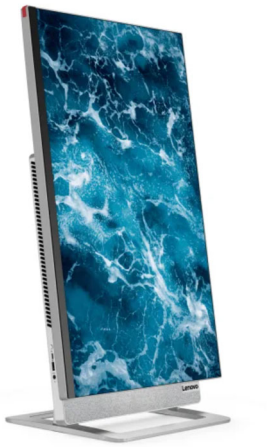
This will be augmented by SOAR (Security Orchestration, Automation and Response) software programs that enable businesses to collect data about security threats, and automatically respond to low-level attacks. We also expect to see more use of UEBA (User and Event Behaviour Analytics) which uses machine learning and deep learning to model the behavior of users on corporate networks and detect behavior that could be the sign of a cyber attack.

 # 5 | Defending aviation from attack Cybersecurity has been spotlighted by the World Economic Forum (WEF) as one of the biggest issues facing the aviation industry. The economic and operational impacts it is currently suffering mean this sector will be particularly at risk over the coming months. The most likely threats to aviation are from the same sorts of threats as other businesses, may they be phishing attempts, data breaches or ransomware. Although cybersecurity is being taken seriously in the boardroom, much work is still to be done to bolster aviation businesses cyber-defenses.

 # 6 | Business Email Compromise (BEC) isn't going away EC will continue to be one of the most financially damaging online crimes and one of the most popular methods for criminal groups to make money. BEC scams exploit the fact that so many of us rely on email to conduct business, both personal and professional. We've likely all been targeted by this kind of attack in the past – an email message that appears to come from a known source making a legitimate request, such as a supplier a company regularly deals with sending an invoice with an updated mailing address. Employees need to be constantly vigilant for this type of attack.

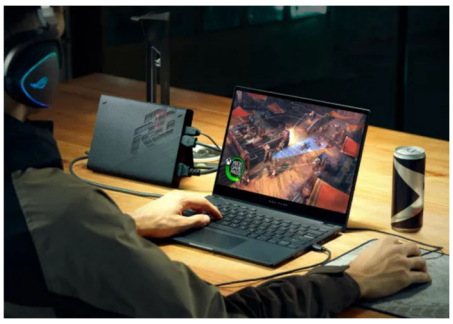
Best CES 2021 Ideas

THE PORTRAIT-MODE PC



Vertically oriented screens aren't just optimized for scrolling through Instagram or Twitter. They're also great for writing or reading digital documents, which is exactly where **Lenovo's Yoga AIO 7** could excel. The all-in-one desktop computer has a 27-inch 4K display with a rotating hinge, so you can flip between landscape and portrait modes like a giant iPad.

PORTABLE PC POWERHOUSE



Why do external graphics cards have to be such hulking monstrosities? Asus doesn't think they do, and has managed to fit Nvidia's mobile RTX 3080 GPU into an enclosure measuring just 8.2 by 6.1 by 1.2 inches. Plug the **ROG XG Mobile** dock into Asus's thin-and-light ROG Flow 13 laptop, and the setup becomes a gaming PC that you can take anywhere.

How to Avoid Misinterpretation when Using Emoji for Business

Here's a tip: *If you're confused while trying to select an Emoji from rows of them, be very cautious.*

Me, thinking who did I send this smiley face to

You wouldn't want to send the wrong Emoji to any of your coworkers. Or to your manager or company CEO. "Make sure that your written words support the intended interpretation of the Emoji," said Hannah Hicklen, a content writer and editor for Clutch. Clutch provides services for businesses, including advertising and marketing, mobile App development, web and software development and more.

Clutch recently surveyed 500 people across the US to learn about their Emoji habits at work. The survey uncovered that communications issues can be caused by improper Emoji use.

Clutch senior product marketer Emily Clark compiled the survey results.

Hicklen said that Emoji use and understanding of Emojis varies by age group. "There's definitely a generation split," Hicklen said. "The age group that most often uses Emojis is 18 to 29." "Even more interesting is that respondents older than 45 said that they felt that use of Emojis isn't professional," she added. "Some even said that they find use of Emojis annoying.

Avoiding Emoji Misinterpretation

Emoji are becoming part of a universal language. That is especially true for the most common ones. When using Emoji in the work environment, small business owners and employees alike should follow these tips:

- Know your audience. Of the 500 companies which responded to the survey, 10 percent don't allow the use of Emojis in work emails. Make sure your employer allows the use of Emojis. Keep in mind who will receive and/or see your email.
- Match the other person's style. If you receive an email or message with an Emoji, it's probably safe to send one in return.
- Stick with the basic Emoji.
- Provide context. The best way to avoid misinterpretation of an Emoji is to include context. Use sentences that support the intended interpretation of the Emoji. Leave no doubt.
- Use for colleagues but not for clients.

Positives of Emoji Use — An Emoji is a face

"It's not the same as face-to-face contact, but it helps people feel connected," Hicklen said. "I've been working remotely and haven't seen coworkers for many months."
"I've found that using Emoji's helps keep the atmosphere relaxed, conversational," she added. "We found in the survey that nearly half of all the employees were using an Emoji as part of a message at least once a day."

Before using an Emoji, think about how you want to present yourself at work, especially to the person who will receive the Emoji. Maintain an awareness of the degree of professionalism which is required for the communication.

"We asked the surveyed people for real-life examples of when their Emoji's had been misinterpreted," Hicklen said. "In one example, the respondent sent an Emoji thinking that it was just a smile – however, the receiver thought the person was flirting."

"Communication issues like this can be a big problem in the workplace," she added. "The use of Emojis can be effective but there can be concerns about interpretation."

"Know your audience, match the recipient's style and stick with basic Emoji's at work," Hicklen said. "Most importantly, provide context to support your intended interpretation of the Emoji."