SIM2K
Adapting Technology to Your Business Needs

February, 2023
Information you can use

SIMformation

Watch Out for Fake SSDs

If you've searched for external SSDs (Solid State Drives) on Amazon.com, you may have noticed something odd: mixed in with the 1TB and 2TB drives from brands like Samsung and SanDisk are a bunch of listings for 16TB SSDs, mostly around $100, and with surprisingly high user ratings. Every single one is a scam, even if they're shipped by Amazon.

The Editor-in-Chief of Review Geek bought one of the "16TB SSDs" and tore it down to reveal a generic 64GB microSD card on a USB 2.0 card reader. Another researcher for ZDNet found the exact same thing. Different packaging and different case colors, but the same trick.

IT experts confirmed that several fake 16TB drives showed up on the first page of results for "external SSD," and over half the results for "16TB SSD" were fakes. The rest were either 16TB enterprise hard drives, multi-drive enclosures, and one actual 16TB external drive, which costs $2,400 and contains two 8TB SSDs. While the top fake had a 3.6-star rating, the next two were 4.8 and 4.2, respectively. How are such obvious fakes getting such high ratings?

It's the scam that Consumer Reports calls "review hijacking." As explained, some third-party sellers take old listings and replace them with new items, leaving the reviews but changing everything else. A quick scan of one fake 16TB drive listing showed five-star reviews for laptop chargers, basketball backpacks, stickers, screen protectors, Mardi Gras beads, and mousepads. The sellers gather good reviews for cheap generic products, swap in a more expensive fake, and then take it down when bad reviews start piling up.

This isn't a new trick. In 2019, an Amazon spokesperson told Consumer Reports they'd spent over $400 million to address the problem in one year alone. "Last year, we prevented more than 13 million attempts to leave an inauthentic review and we took action against more than five million bad actors attempting to manipulate reviews," they said at the time. And yet, nearly four years later, it continues to be an issue.

"The old maxim remains true: if it's too good to be true, it probably isn't," warns IT security experts. "If you're unsure, check the reviews closely. Do they match up to the product? If not, run."

The issue is that knockoff data storage devices pose a particular thread to both corporate and individual computer owners as they may easily corrupt sensitive information and cause permanent data loss.

When it comes to counterfeit solid state drives, there are two main problems users encounter most of all – 1) the actual drive capacity is far different from the claimed one; and 2) the drives use downscale chips which can't provide the appropriate level of data safety.

As a result, tons of crucial files are lost or severely damaged because of wide range of logical and physical failures. Fortunately, there are a few more or less sure ways to spot a fake solid state drive or USB Flash drive and avoid risks to precious files. All you need is to keep in mind the following set of recommendations:

1) Use brand products, keep away from little-known vendors.
These days SSDs manufactured by renowned vendors go with a warranty and proprietary solutions preventing user data from corruption and loss. As for nameless data storage devices, it is better to ignore them in order to avoid possible data-related problems. Still, if you want to use a noname SSD, make sure you have the most recent data backup around. Just in case.
2) Pay close attention to the labels and their shape.
It is not a secret that brand products usually come with lots of specific labels and stickers. Fakers know that for sure. That is why counterfeit data storage devices contain stickers that look really familiar. Fortunately, fake remains a fake in most case. That can be seen from the product labeling: knockoff units usually have pale rectangle labels that have no glossy finish. In addition, a brand logo may look different. When it doubt, try to google for actual brand logos in order to see the difference and avoid falling prey to fakers.
3) Phony data storage devices usually have no special prints with 3D effect on the back.
Brand SSDs usually have serial numbers you can confirm on the manufacturer's website. If the number of your solid state drive is not accepted, that means it's nothing but a fake.
4) Very often counterfeit SSDs feel kind of soft.
They even can bend like rubber. On the contrary, genuine products feel sturdy. So, trusting the tactile impressions makes sense when choosing a reliable solid state drive for the lightning-fast and safe data processing.

Another nasty thing about phony SSDs and USB Flash drives is that no data recovery company, even the most reliable one, cannot guarantee a successful file recovery from questionable data storage device.

Unfortunately, we have had some of our SIM2K clients attempt to buy these products and had less than satisfactory experiences. We will be glad to make purchases for you from properly-vetted sources – give us a call!

Remote Monitoring Scam

Cyber criminals are actively exploiting remote management software to aid phishing scams and steal money from victims, a joint advisory by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) has warned. This comes following the discovery of an e-mail phishing campaign that tricks victims into downloading legitimate remote monitoring and management (RMM) software, which allows attackers to gain access to bank accounts. Crucially, it does so without triggering antivirus alerts because the RMM tool is a genuine application with a verified case for use – and that's something that cyber criminals can exploit as a workaround, rather than attempting to trick victims into downloading malware that could set off warnings.

To date, this campaign is specifically targeting finances, however, the remote access gained means attackers could use it for other malicious purposes such as stealing usernames and passwords, and installing backdoors to compromise systems which could be used to launch ransomware attacks.

The attacks have been ongoing since at least June 2022, and begin with phishing emails designed to manipulate victims. According to the advisory, one common phishing template being leveraged in these attacks is a message that claims an annual subscription is about to be automatically renewed at a cost of hundreds of dollars. This is designed to panic victims into calling the "help desk" listed in the e-mail. If they do this, the scammer-run "help desk" will attempt to convince the victim to download remote management software to 'help' them with their query and cancel the payment. But in reality, no payment is about to occur and all the attackers want to do is convince the victim to log in to their online bank account while the remote management software is active. The attackers use this access to the bank account to steal money from the victim.

In this campaign, the attackers are using ScreenConnect and AnyDesk, but the advisory warns that they can use any legitimate remote management software. And because attackers can download legitimate RMM software as self-contained, portable executables, they can bypass both administrative privilege requirements and software management control policies.

"Threat actors often target legitimate users of RMM software. Targets can include managed service providers (MSPs) and IT help desks, who regularly use legitimate RMM software for technical and security end-user support, network management, endpoint monitoring, and to interact remotely with hosts for IT-support functions," warns the advisory.

According to CISA, actions that can be taken to help avoid falling victim to this and similar campaigns include implementing best practices to block phishing e-mails, and to carefully monitor activity to identify suspicious or unwarranted use of software on the network. The agency also suggests implementing a user-training program and running phishing exercises to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments.

SIM2K offers training as described above, and while RMM is one of the tools our Support team uses, we would never initiate a remote session via e-mail, more for an active trouble-shooting look at an issue with your participation and authorization. Call us if you have concerns about any connection requests.

Malware Targets Zoom

A recent malware attack on Zoom users that aimed to steal private banking information has been shut down. The malware was identified by experts at Cyble Research & Intelligence Labs, and while it has been reported that the website hosting the malicious download is no longer available, experts are warning Zoom users to watch out for future attacks.

The malware known as IcedID has been put into action through threat actors actively spreading it by using modified versions of the Zoom application. This has affected hundreds of businesses, as Zoom has grown immensely in popularity, especially among companies that transitioned to working from home at the start of the COVID-19 pandemic in 2020. The malware acts as a loader (a type of malware that is used to install other malware onto a computer) by stealing private information from these companies and dumping additional malware onto their employees' computers.

This means that it is stealing sensitive information and also potentially installing other harmful software that can cause further damage. This can cause significant harm to the affected businesses, as they may lose valuable information and suffer from additional security breaches or system disruptions.

Aside from being a loader, IcedID can also download additional modules from the internet and deliver other malware families, making it significantly difficult for the user to get rid of the malware once it's planted into a computer. Once downloaded, its primary purpose is to steal private banking credentials.

The most common way IcedID had been spread among users is by appearing via spam e-mails. The malware is hidden in e-mail attachments found within malicious office files. However, these Zoom hackers tried a new technique that many were unprepared for this time around. They use a phishing website called explorezoom.com to deliver the malware. This is a fake website dsisguised as an official Zoom domain whose sole purpose is to deliver the IcedID malware. The page tells users that to use Zoom, they must download a file called ZoomInstallerFull.exe. The file will download the actual Zoom application to distract the user from realizing that IcedID malware is also being downloaded onto their device.

If your company uses Zoom, be sure your employees are aware of this scam and to report any suspicious spam e-mails directing them to the website (which may surface as a new domain, given the "whack a mole" tendency for cybercrooks to repeat successful ploys under a new name). A good anti-virus program and endpoint protection should also help to protect against this sort of malicious software downloads. SIM2K continues to refine our security suite to protect you and stay ahead of the "bad guys." Call us if you have concerns about your malware protection.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

When is a Hack not a Hack?

A security breach involving T-Mobile generated a significant amount of media coverage last week. The incident, which involved a person or group accessing non-personal information of about 37 million customers, was compared to previous security breaches in which T-Mobile found itself the victim of several large-scale cyberattacks that resulted in serious, sensitive customer information leaked on the Internet, one that triggered at least two class action lawsuits against the company.

The latest security incident generated headlines coloring the episode as an "attack," leading many to believe that T-Mobile was on the receiving end of compromise similar in nature to what the phone company has faced over the last several years. ABC News, USA Today and CNN among others all stated that the 37 million customers data was "hacked."

But this latest security incident was not a hack in the conventional sense. The "bad actor" that T-Mobile blamed for the incident simply exploited a door that T-Mobile left open for some legitimate purposes, and used it to harvest data of millions of customers. Instead, the "bad actor" – who may have acted alone, or might be connected to a larger group – used an application programming interface (API) to access some customer data in a way that went beyond what the company intended. Simply put, APIs allow developers to access certain parts of another website or service when they're building out their own applications.

T-Mobile hasn't explained why non-sensitive customer information like names, home addresses and phone numbers were available through an API, but it could have been for any number of reasons. It could have been connected to social media-based customer service, where users are asked to authenticate themselves as a T-Mobile subscriber when seeking help through Twitter and Facebook. It could have also been part of T-Mobile's external sales efforts, where some customer information is sold to third parties for purposes of marketing sand advertising.

What is known is that the person or group T-Mobile is calling a "bad actor" first started accessing the company's API and collecting data around November 25 of last year, and continued accessing the API and collecting data until the company became aware of the practice on January 5.

While the media suggested T-Mobile was the victim of a sophisticated cyberattack, the reality of the situation is actually pretty boring: T-Mobile was not careful in deciding who got access to an API. The "bad actor" didn't need to do anything elaborate like guess a username and password or force their way in – they simply connected to T-Mobile's API, as anyone could have done, and grabbed the data that was freely available to take.

To T-Mobile's credit, it never characterized the incident as a "hack." But the reality of what happened – that someone walked through an open door and grabbed whatever was there to take – requires a serious shift in conversation. Why was that information available to take? Why didn't T-Mobile better scrutinize who could access its API, and offer a limited set of conditional access to that effect? As long as reporters dismiss the breach as a "hack," those questions probably won't be answered. And T-Mobile customers (your editor included) are wondering if any of our personal information is now out there on the "dark web" and subject to further cybercriminal activities. T-Mobile said affected customers will be notified, so be watching for further information and any remediation steps T-Mobile may take.

"Random Tid-Bytes"

Amazon and other Tech Company Layoffs

Amazon has confirmed that company layoffs will total more than 18,000 employees, with the bulk of job cuts coming later in January. While several teams are impacted, the majority of the job cuts will be in the Amazon Stores and People, Experience, and Technology organizations. The layoffs, which represent the largest round of job cuts in the company's history, are a result of "the uncertain economy," said CEO Andy Jassy. He added that Amazon had weathered "difficult economies" in the past and would continue to do so. The layoffs come after a hiring spree during the pandemic, as lockdowns and other precautions caused consumers to turn to online shopping, fueling Amazon's retail business. As the new year unfolds, tech companies continue to make job cuts. Salesforce announced it will lay off about 10% of its workforce, roughly 8,000 employees, and close some offices as part of a restructuring plan. Phillips has laid off 6,000 workers, and PayPal has announced 2,000 employees will be laid off. So far in 2023, there have been 272 layoffs at tech companies with 86,882 people impacted, according to a tech layoff tracker. In 2022, there were 1,517 layoffs at tech companies with 237,874 people impacted.

New SEC Regulations Released

The Securities and Exchange Commission is proposing new rules under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 to require registered investment advisers and investment companies to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks. The Commission also is proposing a new rule and form under the Advisers Act to require advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission. With respect to disclosure, the Commission is proposing amendments to various forms regarding the disclosure related to significant cybersecurity risks and cybersecurity incidents that affect advisers and funds and their clients and shareholders. Finally, the SEC is proposing new recordkeeping requirements under the Advisers Act and Investment Company Act. The proposed rules would increase the prominence of required disclosure of cybersecurity incidents in several corporate filings, including annual and quarterly filings and current reports. The proposal would also require disclosure of a registrant's policies and procedures to identify and manage cybersecurity risks; management's role in implementing cybersecurity policies, procedures and strategies; as well as the board of directors' oversight and expertise. So if your company is under SEC oversight, be prepared to increase your cybersecurity profile and have prepared a policy to address this. SIM2K can assist with drafting cybersecurity policies and rules tailored to fit your company's activities.

Apple Vulnerability

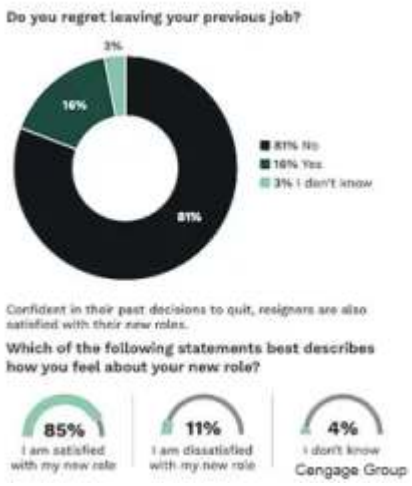
Apple has now released security content for iOS 12.5.7. which includes a patch a vulnerability. This covers: iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, and iPod touch (6th generation). Apple says the vulnerability is processing maliciously crafted web content which may lead to arbitrary code execution – an attacker can try to lure his victims to a malicious site to compromise their devices. But Apple has not disclosed any details about the circumstances under which the vulnerability was actively exploited. If you have an older iPhone, be sure to upgrade your iOS. Call us if you need help determining what version of iOS you are running or to upgrade your device.

The Great Resignation and Tech Workers

Tens of millions of American have quit their jobs since the beginning of the pandemic in what's become known as the Great Resignation – and a new study indicates those workers feel good about where they wound up.

The study by online education service Cengage Group shows "the Great Resigners" are generally happy about their workplace decisions, with an average 81% indicating they do not regret leaving their previous job. The survey was conducted in November as a follow-up to research conducted exactly a year earlier. Cengage surveyed workers who quit to better understand their current job satisfaction, whether they switched industries, upskilled, or trained to start new roles, for example. Additionally, Cengage wanted to capture how inflation, a potential recession, and a string of tech layoffs affected workers.

Not only did those who quit not regret leaving their previous jobs, but 85% indicated they're satisfied in their new roles. Only a small percentage (6%) are considering returning to their previous job. The Cengage figures contradict other studies that found more workers who quit were unhappy after doing so.



Over the course of 2021, more than 47 million people quit their jobs, representing 23% of the total U.S. workforce, according to the Bureau of Labor Statistics (BLS). And in 2022, roughly 38 million more quit. The Great Resignation, which began around April 2021, has seen more than four million US workers quitting their jobs every month. While numbers began to tick down slightly in September 2022, the latest data from the US Bureau of Labor Statistics showed 4.17 million people quit their jobs in November. That high-level churn is far from over, even if some high-profile layoffs have been dominating news in recent weeks.

"While the recent layoffs certainly impact the balance of power, especially for those at big tech companies, in my view the tech sector is very much a perennial candidate's market," said a Cengage spokesman. "With the quick pace at which technology advances, there is always a need for new skills and new talent. The tech industry isn't the only market for tech talent. There is demand for technologists in every single industry and we're seeing talent being scooped up by startups and enterprises in other industries."

One of the main reasons organizations are struggling to fill vacancies — 200,000 of those open positions are in IT — is a shortage of people with the right skills (45%) ahead of inability to match expectations of flexible work models (39%), according to data from research firm IDC.

One of the top consequences of the Great Resignation was an increased workload on remaining employees (52%), according to IDC. IDC's Future of Work group said its data shows people quit their jobs over the past two years for five main reasons:

- They were doing the work of those who left without backfill or training at times.
- They needed better work-life balance brought on by pandemic pressures and new lifestyles.
- They had new job opportunities in the same or different fields.
- There were opportunities to be self-employed, start a new business, or become a gig worker.
- Their proximity to retirement and a reluctance to shift to new ways of working prompted them to retire early.

The continued turnover of employees – despite concerns of a looming recession and high inflation – suggests tech talent and others aren't regretting their decisions to leave, according to IDC.

So, where did all the quitters go? In Cengage Group's 2021 survey, those who quit were asked if they planned to stay in the same industry or make a change; their responses were almost a perfect 50/50 split on what they planned to do. In 2022, the same scenario played out: half switched industries and half stayed in the same industry. One in five quitters (21%) who switched careers chose technology as their new career, according to the survey.

Tech workers were more likely to be satisfied with their new roles than those in other industries, according to Cengage. For example, 86% of technology workers indicated they're satisfied with their new jobs, compared to 69% of healthcare workers who were happy.

Despite the findings by Cengage, other surveys have shown that employees who quit over the past few years regretted the decision. For example, human resources and payroll services provider Paychex recently released survey results from 800 employees and 300 employers that showed eight of 10 workers who quit during the Great Resignation regretted it, including an overwhelming 89% of Gen Zers.

Only about half of Paychex's survey respondents indicated they're satisfied with mental health (54%) and work-life balance (43%) in their new workplace, with Gen Zers reporting the lowest levels of positive mental health and work-life balance. Sixty-eight percent of employees attempted to get their jobs back, but only 27% of employers have rehired employees that left during the Great Resignation, according to Paychex.

A survey of 2,500 workers from The Muse "found that almost three-quarters of workers (72 percent) experienced either 'surprise or regret' that the new position or new company they quit their job for turned out to be 'very different' from what they were led to believe. Nearly half (48 percent) of these workers said they would try to get their old job back."

And a poll commissioned by USA Today found that just 26% of job switchers liked their new job enough to stay.

So, who to believe? In the US, more than 5.6 million jobs went unfilled in October 2022, according to the BLS, and unemployment has hit a 50-year-low, remaining between 3.5% and 3.7% for most of 2022. In technology, unemployment is just 1.8%.

The upshot: regardless of whether employees were happy with their job change, they've still got plenty of options.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com