TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

September 2020

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

FORMER UBER SECURITY CHIEF CHARGED IN 2016 HACK COVER-UP

The former chief security officer of Uber Technologies, Joseph Sullivan, has been charged with obstruction of justice for his alleged role in the cover-up of the 2016 hack of the company. This is according to a press release from the Office of the United States Attorney in Northern California. The charges relate to the security incident in which Uber was hacked, and roughly 57 million individuals' data was exposed. The database information contained personal information about drivers and customers, including more than 600,000 drivers license numbers of Uber drivers.

The case brought against Sullivan alleges that the former Uber CSO actively impeded the Federal Trade Commission's investigation. The specifics can be found in the following excerpt from the press release:

More on next page...

"Rather than report the 2016 breach, Sullivan allegedly took deliberate steps to prevent knowledge of the breach from reaching the FTC. For example, Sullivan sought to pay the hackers off by funneling the payoff through a bug bounty program — a program in which a third party intermediary arranges payment to so-called "white hat" hackers who point out security issues but have not actually compromised data."

It was not until new management took over Uber's operations that the breach was disclosed in full. It was at that time that the company began fully cooperating with federal investigators. Sullivan was fired by the new management in 2017.

Leading the case is United States Attorney David L. Anderson and FBI Deputy Special Agent in Charge Craig D. Fair. They allege that Sullivan also actively sought to deceive the new management in an attempt to uncover his misdeeds. If these allegations are proven and Sullivan is convicted, he faces up to eight years in prison.

The court date has not yet been determined, but as developments emerge, they will be reported on.— *Derek Kortepeter for Techgenix*

IT'S OFFICIAL: MICROSOFT SHUTS DOWN WINDOWS FOR MOBILE

Microsoft's Windows for Mobile platform is now officially dead. While it already died a while ago in terms of sales, the support page on Microsoft has made it official. Microsoft has stopped releasing security and software updates for all Windows mobiles effective Dec. 10. All technical support for the devices also ended on the same date and, which means no smartphone running Windows 10 mobile version 1709 will receive updates.

Here's part of the official announcement from Microsoft:

"*With the Windows 10 Mobile OS end of support, we recommend that customers move to a supported Android or iOS device. Microsoft's mission statement to empower every person and every organization on the planet to achieve more, compels us to support our Mobile apps on those platforms and devices.*" *— More on the next page*

What about existing Windows mobile users?

As for those who still use Windows mobiles as their primary device, Microsoft has announced that they can back up all the essential data and some apps until March 10, 2020. Moreover, some features such as photo uploads and restoring a Windows device from an existing device's backup will continue to work until the end of 2020.

While the support for the devices has ended, users will still be able to continue using their Windows devices. However, some of the OS-based features are going to be affected in terms of usage after Dec. 10.

Should you still use Windows mobile?

Although users will still be able to use their Windows mobile devices, it is not a good idea. Any smartphone that doesn't receive timely security updates is vulnerable to cyberattacks. Considering the surging number of cyberattacks globally, users who continue with Windows mobiles open themselves up to serious cyberthreats.

A quick recap

The first-ever Windows OS-powered handsets were launched in the year 2011. These smartphones were originally designed and marketed by Nokia as the Nokia Lumia series of smartphones. In 2014, Microsoft acquired the Lumia series from Nokia and started to phase out Nokia's name from the branding. Microsoft then started selling the Lumia devices under the Microsoft name. While the demand for these devices was decent in the initial days — thanks to the reputation of Windows OS for PCs — it soon started to fall sharply. Microsoft stopped selling Lumia devices in Microsoft stores by the end of 2016.

With the users dropping in millions, Microsoft confirmed in October 2017 that they would no longer manufacture or sell any Windows OS-based smartphones. While it is obvious the number of Windows mobile users have been falling sharply, there still are a few users who are longing on to Windows handsets. And this announcement from Microsoft is exactly for them.— *Sukesh Mudrakola for Techgenix*

UNIVERSITY OF UTAH HIT BY RANSOMWARE ATTACK, PAYS RANSOM

The University of Utah has released a notice updating its community of faculty and students on a major ransomware incident. According to the notice, released Aug. 20, the University of Utah's College of Social and Behavioral Science (CSBS) "experienced a criminal ransomware attack, which rendered its servers temporarily inaccessible." This incident took place on July 19 and caused roughly .02 percent of the data on the servers to be compromised. This data included personal data on faculty and members of the student body. The notice states that a vulnerability was to blame for the ransomware infecting the servers.

On July 29 (10 days after the ransomware attack) the University of Utah sent out a campus-wide notice to all members of the community, instructing them to change their passwords. The University of Utah stated that the order to change passwords came so late due to law enforcement's suggestions during the investigation, namely that "preparations had to be made to ensure that password resets went smoothly in each campus entity."

The notice did not reveal who was responsible for the ransomware attack, but the University of Utah admitted it paid the ransom to the tune of $457,059.24. The money came from a cyber insurance policy. No other funds, such as tuition, were used to pay for the ransom, the University said.

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-8324 x2

In a statement to Threatpost's Lindsey O' Donnell, a University of Utah spokesman stated that they received the ransomware decryption key upon payment. They also had this to say about paying the ransom:

"*However, it [the decryption key] was not a primary consideration in paying the ransom... We were able to recover almost everything from backups, but it is useful to have the ability to decrypt and recover files created after the last backup... We continue to parse the information that was stolen, and we will update the [press release] with the findings of the analysis once it is completed... While the attackers stole a small amount of data relative to the total number of files stored, there are still many documents to examine thoroughly.* "

The official position of most security professionals is that paying the ransom during a ransomware incident is the wrong move. What's done is done in this case, but all the University of Utah has done is likely to encourage its attackers to strike again. There is no guarantee that they, whoever it was behind the attack, will not come back for seconds. Additionally, there is never a guarantee that attackers will hand over the decryption key once paid.

Ransomware is here to stay, so it is vital that organizations around the world move to a unified, effective strategy to counter the inevitable attacks. Universities, in particular, are experiencing an uptick in ransomware attacks. As such, they should implement the strategies soon.—*Derek Kortepeter for Techgenix*

Client Spotlight

Baker Barrios

Baker Barrios Architects has a long-standing commitment to values and ideals that will forever be imprinted on our legacy and woven into the very DNA of the company. We are in the **business** of **service**. Through our commitment to meaningful relationships, both internal and external, we are proud to produce creative work that inspires communities around us while making lives better. That's how we started and that's how we'll continue to grow. Some things – like our values and ideals – should never change.