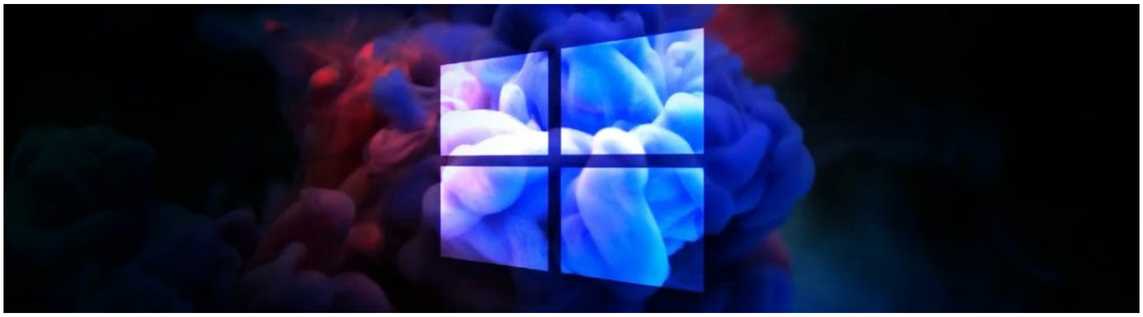
Talk Nerdy To Me

April 2022

Windows 11 Gets A New Desktop Watermark On Unsupported Hardware



Microsoft is pushing ahead with plans to warn Windows 11 users that have installed the operating system on unsupported hardware. In a new update to Windows 11, a watermark has appeared on the desktop wallpaper for unsupported systems, alongside a similar warning in the landing page of the settings app.

Microsoft had been testing these changes last month, but they're now rolling out to Release Preview just ahead of a full release to all Windows 11 users in the coming days. While Microsoft doesn't mention the addition of a watermark in its "improvements" list for this update, testers have noticed it's included.

If Windows 11 is running on unsupported hardware, a new desktop watermark will state "System requirements not met. Go to settings to learn more." It's similar, but far less prominent, to the semi-transparent watermark that appears in Windows if you haven't activated the OS.

It's been possible to bypass Microsoft's minimum hardware requirements for Windows 11 and install the operating system freely. The controversial hardware requirements mean Windows 11 only officially supports Intel 8th Gen Coffee Lake or Zen+ and Zen 2 CPUs and up, leaving millions of PCs behind. Anyone that has used the workaround will now start to see this warning in Windows 11.

Microsoft has used similar warnings for unactivated versions of Windows in the past, and restricts features like dark mode, personalization settings, and themes from being modified until a system is activated. Microsoft doesn't appear to be experimenting with any similar feature restrictions, and the desktop watermark can likely be disabled with some registry changes.

Source: https://www.theverge.com/

What Is Smishing And How To Defend Against It?

A nefarious text message could be on its way to a smartphone near you. This is a message, often purporting to be from your bank asking you for personal or financial information such as your account or ATM number. Providing the information is as good as handing thieves the keys to your bank balance.

Smishing is a portmanteau of “SMS” (short message services, better known as texting) and “phishing.” When cybercriminals “phish,” they send fraudulent emails that seek to trick the recipient into opening a malware-laden attachment or clicking on a malicious link. Smishing simply uses text messages instead of email.

In a nutshell, like most cybercriminals, they are out to steal your personal data, which they can then use to steal money—usually yours, but sometimes also your company’s. Cybercriminals use two methods to steal this data. They might trick you into downloading malware that installs itself on your phone. This malware might masquerade as a legitimate app, tricking you into typing in confidential information and sending this data to the cybercriminals. On the other hand, the link in the smishing message might take you to a fake site where you’re asked to type sensitive personal information that the cybercriminals can use to steal your online ID.

As more and more people use their personal smartphones for work (a trend called BYOD, or “bring your own device”) smishing is becoming a business threat as well as a consumer threat. So it should come as no surprise that, according to Cloudmark, smishing has become the leading form of malicious text message.

The good news is that the potential ramifications of these attacks are easy to protect against. In fact, you can keep yourself safe by doing nothing at all. The attack can only do damage if you take the bait. There are a few things to keep in mind that will help you protect yourself against these attacks.

You should regard urgent security alerts and you-must-act-now coupon redemptions, offers or deals as warning signs of a hacking attempt.

No financial institution or merchant will send you a text message asking you to update your account information or confirm your ATM card code. If you get a message that seems to be from your bank or a merchant you do business with, and it asks you to click on something in the message, it’s a fraud. Call your bank or merchant directly if you are in any doubt.

Never click a reply link or phone number in a message you’re not sure about.

Look for suspicious numbers that don’t look like real mobile phone numbers, like “5000”. As Network World notes, these numbers link to email-to-text services, which are sometimes used by scam artists to avoid providing their actual phone numbers.

Don’t store your credit card or banking information on your smartphone. If the information isn’t there, thieves can’t steal it even if they do slip malware onto your phone.

Refuse to take the bait—simply don’t respond.

Report all smishing attacks to the FCC to try to protect others.

Remember that, like email phishing, smishing is a crime of trickery—it depends on fooling the victim into cooperating by clicking a link or providing information. Indeed, the simplest protection against these attacks is to do nothing at all. So long as you don’t respond, a malicious text cannot do anything. Ignore it and it will go away.

Source: https://usa.kaspersky.com/

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

Meet Caleb Harter

Meet Caleb Harter!

Caleb is our new intern. He graduated high school early this year and decided to help us out until he heads off to realtor's school!

Caleb enjoys playing video games, shopping with his girlfriend Aubree, and drive in movies.

Welcome to the team!

Grabbing The Bull By The Hornes - Preferred IT CEO, Jason Horne, Is Gaining Ground Fast

Check out Preferred IT Group's CEO, Jason Horne in MSP Success Magazine!

"So, in the sports bar that night, where patrons sampled cold beer and cheered on the Cubs and Komets, a vision for what would become Preferred IT emerged."

MSP SUCCESS
MAGAZINE
Grabbing The Bull By The Hornes
Preferred IT CEO, Jason Horne, Is Gaining Ground FAST
Page 14
Marcus Lemonis Reveals
Now Is The Time To Double Down On Marketing
Page 22
LANDING YOUR MOON SHOT
Buzz Aldrin Talks About Hitting BIG Goals
Page 8
Determination That Won't Quit
Shark Tank's Barbara Corcoran's Rise To New York Realty Royalty: How You Can Dominate Sales Like The Queen
Page 17
MSP SUCCESS
Special Edition: Winter 2022
MSPSuccessMagazine.com
Jason Horne, Co-Founder Of Preferred IT Group

FUN FACT!

92% of the world's currency exists only on computers

preferred IT group

preferred IT group

CONTACT US

Fort Wayne	Warsaw
260.440.7377	**574.306.4288**
Columbia City	**Indianapolis**
260.213.4266	**317.426.8180**

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.