BANC OF CALIFORNIA | TOGETHER WE WIN®

YOU CAN BANC ON IT

QUESTIONS WE NEVER ASK

WHEN YOU KEEP COMPUTER SOFTWARE UPDATED, YOU KEEP INTRUDERS OUT

The PCs your employees use are potential open doors to your network. Those PCs need ongoing security updates to keep intruders out.

In previous Business Insights articles, we explored the topic of "questions we never ask." However, there are some questions we feel we need to ask, or least present to our clients. One of them is this:

Is the computer you're using right now current with the latest updates to its operating system? In other words:

- If you're using a PC that has Windows 10 installed, does it have the latest updates?
- Is the version of Windows you're currently using still supported by Microsoft, as far as security updates are concerned?
- Should you be upgrading (not updating) your operating system?

The critical business of computer security.

If your business isn't in the hardware, software or networking industries, it's understandable if you're not familiar with computer technologies and security issues. Still, it's important for every business to make computer security a top priority—along with the other cybersecurity issues we've presented so far, such as password security, multifactor authentication and so on.

Computer security and protection can't be overlooked. Hackers are aware of weaknesses in Windows, and often they're typically the ones who find them. Worse yet, they actively seek to exploit the flaws they find. Microsoft does its best to release security updates (or patches) to Windows to fix any flaws they discover themselves or become aware of.

Windows, which accounts for 80% of computer user operating systems, is amazingly complex...but it isn't 100% perfect. Every version that is released initially has flaws (vulnerabilities) that the security patches help to fix. If a business doesn't install the updates, its computers are at risk.

And that risk is significant.

The threat of malware.

Malware and ransomware have become a major problem for organizations of all kinds across the globe. International corporations, government agencies, schools and hospitals have become victims of significant and successful attacks.

Even if your company isn't an industry leader, a network attack could devastate your business.

One prime reason an attack happens is because a business doesn't install updates to its operating system and software. Hackers are well aware of Windows' potential weaknesses, and they exploit the loopholes on unprotected computers.

It's important to update Windows on business PCs on a regular basis. Those updates from Microsoft patch flaws in the operating system that hackers discover and eventually exploit. That's how they gain access to computers and networks.

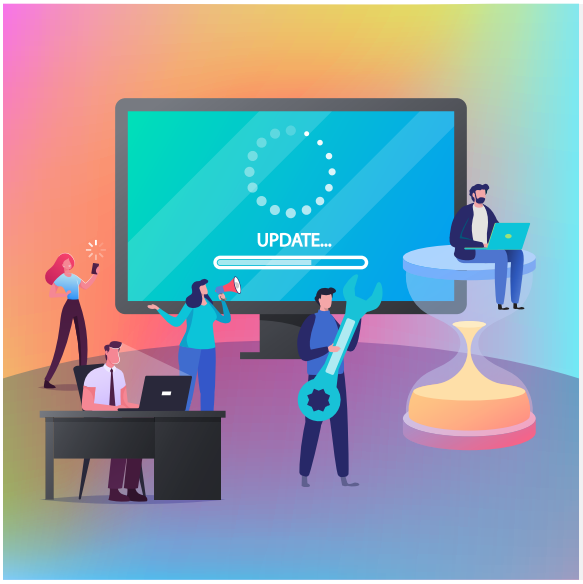
SPOT THE RED FLAGS. AVOID A SCAM.

One of the things they do is install malware. Hackers move fast and act without a care and conscience. If they come across networks that aren't protected with the latest operating system patches, that's where they'll focus their attention.

Protecting your investments.

Windows updates are necessary, even if they seem like a burdensome task and are easy to ignore or put off till later. It's not a complicated process, and the few minutes spent are well worth it. Often, updates are included for other features related to the operating system, but security updates are the most important to obtain.

In case you're not aware of it, there is no fee for updates and the fixes are available to EVERY user of Windows. However, it's up to everyone—from business owners to employees—to 1) stay on top of available updates, 2) install the patches and 3) update their version of Windows.



An important step to take.

If your business has an IT department or IT specialist, they should be assigned the task of first inventorying all computers that connect to your company network and systems. The most important step is installing the most recent Windows security updates.

Banc of California offers additional cybersecurity information for small- to medium-size businesses on the Business Insights page on our website. The resources include Cyber Readiness Guides for IT professionals as well as business leaders.

The bottom line is simply this: It's important to keep all the software on your computers up to date to avoid problems, especially those caused by external attacks. In the same way our vehicles need tune-ups to run smoothly and efficiently, our technological tools need regular servicing too, to work at peak performance.

To read more Business Insights articles, please visit: **bancofcal.com/business-insights**