

Stop Abbreviating 2020 and Essential Tech Tips for the New Year



While you work on those resolutions to eat right and exercise, make a few resolutions for your business, as well. A fresh year presents the perfect opportunity to tighten security and run some much-needed maintenance. Protect your business with these basic tech tips for the new year.

1. Stop Abbreviating 2020

Commit now to writing out all four digits of the year. Writing "20" instead of "2020" leaves the door open for fraudsters. For example, suppose you sign a credit contract with the date 1/27/20. A bad actor could change the date to 1/27/2019 and attempt to collect an additional year of payments.

The same logic applies to uncashed checks. If someone finds an uncashed check next year, he could change the date to read 2021 and cash the check months after its expiration.

2. Say a Final Good-bye to Windows 7

Microsoft has now sunsetted its Windows 7 operating system. This means that, as of January 14, Microsoft no longer provides security updates and support for the product. Unfortunately, many businesses still have machines running Windows 7, leaving them extremely vulnerable to cyber attacks.

Look through your business for any computers running Windows 7. And put upgrading to Windows 10 at the top of your priority list of tech tips for the new year. You cannot afford to leave a door open into your network.



3. Update Your Password Policy

While experts no longer recommend frequent password changes, strong passwords remain the first line of defense for protecting valuable data. Make sure your corporate [password policy](#) includes specific rules to guide users.

For example, passwords should be long and should never include personal information such as birthdates. Passphrases work well. And users should never use the same password for multiple accounts. Consider using a password manager to store company passwords in a secure, central location and reduce the need to remember dozens of passwords.

4. Ensure Frequent, Reliable Backups

Double-check your backups to ensure they work properly. If you have not already done so, set backups to run automatically on a frequent, regular basis. Store at least one copy of the backup off-site, or at least not connected to the network. Keep the backup safe by encrypting it and test your backups periodically.

Individual users should back up all devices regularly. This includes desktop PCs, laptops and mobile devices. Reliable backups provide the key to recovering quickly from ransomware attacks and other disasters.

5. Install Updates to Software and Firmware

If you have delayed installing security updates to your software or firmware, do it now. Those updates form a critical part of your security program. Where possible, set updates to install automatically.

6. Check Your Website

For many potential customers, your website offers an important first impression for your business. If you have not updated your website in a while, now may be time for a facelift. SEO optimization guidelines and web technology change quickly. Refresh your [website design](#) for increased user engagement.



7. Check Your Compliance Status

Important new [data privacy laws](#) take effect in California and New York in the first quarter of this year. Consequently, businesses can no longer afford to put privacy concerns on a back burner. Conduct an inventory of the privacy laws that apply to your industry, identify any gaps and begin implementing a compliance strategy.

We'll Help You Implement Tech Tips for the New Year

eMazzanti Technologies has a team of experts ready to help you incorporate these tech tips for the new year into your organization. So, stop abbreviating 2020 and we'll help you with the rest. From tightening up your [security and privacy strategy](#) to refreshing your website design and [digital marketing](#), we have you covered.

2015 | 2013 | 2012 Microsoft
Partner of the Year



Inc. 500 || **5000**
2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010



ShoreTel Sky
Partner of the Year