JANUARY 2020

DigeTekS LLC

di•ge•ra•ti *persons well versed in computer use and technology*

IT Consulting | Managed Services | Network Security | Hosted Services

Phone Support:
(855) 536-5052 x1

Email Support:
supportrequest@digeteks.com

Remote Support:
www.digeteks.com

Please don't hesitate to submit a ticket if you have an issue!

You can call our help desk support line, reach out to us through our remote support link on our website, or send us an email at supportrequest@digeteks.com.

PC Tips & Tricks:

1. Is your PC giving you issues? Try a simple restart! Restarting your computer is often one of the first troubleshooting steps.

2. Encrypt your laptop's hard drive to prevent access to your data in the instance your machine is lost/stolen. You can encrypt your mobile phone, too!

3. It's never a bad time to do a little PC file spring cleaning. Removing/storing old unused files elsewhere can help improve the performance of your machine.

4. Whether it's to the cloud or an external drive, backup your computer's data regularly to safeguard data loss.

H4PPY N3w Y3@R!

Snatch Ransomware | Safe Mode Trick

A new strain of ransomware is sneaking past anti virus programs by running its encryption process in Windows Safe Mode. Most anti virus programs don't start in Safe Mode, so Snatch initiates a Safe Mode boot up where it can initiate encryption undetected. It's only a matter of time until other ransomware developers employ this trick...

When was the last time you reviewed your cybersecurity defenses and disaster recovery plan?

Ring Home IoT Device Security

Internet of Things (IoT) devices like smart doorbells can leave your home network and overall privacy vulnerable. If you have a Ring device, be sure that the password/email combination you use is entirely unique (aka never been used before by ANY other account) and that you have 2 Factor Authentication (2FA) enabled in the settings. At this point in time, Ring users aren't notified about suspicious logins and hackers have been publishing thousands of credentials on the dark web as of lately.

Time to Review Holiday Shopping Charges

Now that the holidays are over, don't forget to look over all accrued credit card charges. Because of unencrypted payment fields, POS malware, data breaches, and other risks during the shopping season, ensure that there's no suspicious activity. In general, it's always a good idea to review statements as they're released to mitigate fraud.

What's Your New Year's Resolution?

New year, new you. Here are 10 awesome and achievable goals to set for yourself this year:

1. Never use an email-password combination that you have *ever* used before.
2. Use passwords that contain symbols, uppercase letters, lowercase letters, and are 8 or more characters long.
3. Always verify suspicious email requests and never blindly click on links or attachments.
4. Backup your local data every month (at least).
5. Always use MFA for accounts that offer it.
6. Never plug random drives into your devices.
7. Always lock your devices when you're not using them.
8. Keep food and drinks away from your devices.
9. Never procrastinate security updates.
10. Restart your computer every week (at minimum).

Do you know your company's Encryption Policy?

In order to protect confidential and sensitive information, your employer may require you to encrypt any electronic device (such as a PC, laptop, or cell phone) used to access or store company data.

Review with your manager if you have any questions or concerns.

DigeTekS Is Partnered With: SEP Citrix Micro Focus Microsoft SUSE WatchGuard McAfee