JANUARY 2019

DigeTekS LLC

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

IT Consulting | Managed Services | Help Desk Support | 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 suport line, reach out to us through our remote support link on our website, or send us an email at supportrequest@digeteks.com.

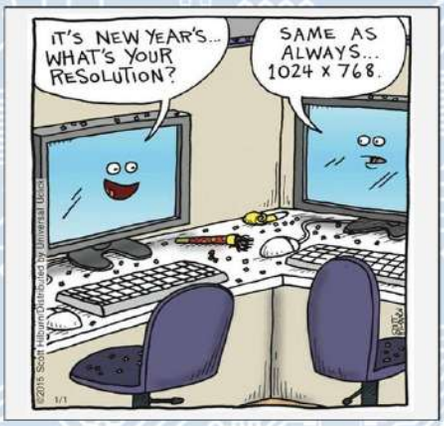
PC Tips & Tricks:

1. When in doubt, ask your IT team!

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. Use a VPN (Virtual Private Network) while using free public WiFi to keep your web activities private.

4. Whether it's to the cloud or an external drive, backup your computer's data regularly to safeguard data loss in the instance of a ransomware attack or hardware disaster.



HAPPY NEW YEAR!

New Year New Threats

We may not know what new security threats we will encounter this year, but we do know that the best approach to protecting data is a proactive one. What are you doing to protect your clients' information from the many cyber threats of today? We recommend performing penetration testing and reviewing practices and policies with employees at least once per year.

Facebook API Bug Exposed Private Photos

Facebook allows users the ability to mark certain photos or albums private. Unfortunately, last month a Facebook API bug allowed 1,500 apps the ability to access the non-public photos of up to 6.8 million Facebook users. Those who installed any of the 1,500 apps were notified and the bug has since been fixed.
Where do you store your private photos? If you have photos that absolutely shouldn't been seen by anyone but yourself, we recommend storing these offline on an external drive. An external drive is also a great means of backup in addition to the cloud.

Over 20,000 WordPress Sites Infected

Do you have a WordPress site? Hackers have infected over 20,000 sites by using a script that automatically generates a range of usernames and passwords. The brute-force method has allowed hackers to enslave (and continue to enslave) thousands of sites.
The simplest way to protect your WordPress site(s) is to use a complex password. An example of a complex password is "!Y0u$hallN0TP@$S!". Additional measures to protect your site(s) include keeping your WordPress install up to date, employing multi-factor authentication (MFA or 2FA), and restricting admin account access to specific IP addresses.

Marriot Starwood Data Breach

Have you stayed at a Marriott owned Starwood property on or before September 10, 2018? Hackers had unauthorized access to Marriot's Starwood network since 2014 that allowed the personal information of 383 million guests to be stolen. Over 5 million unencrypted passport numbers have been confirmed stolen and although it is not known if hackers have been able to decrypt stolen billing info, it's recommended that you freeze your credit (until needed) to combat the risk of identity theft.

Do you know your company's Email Retention Policy?

Some industries, such as healthcare and banking, are legally required to retain emails for a certain amount of time before deletion, while others may employ an Email Retention Policy for improved email management efficiency and more.

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

CITRIX Microsoft MICRO FOCUS SUSE NetIQ McAfee vmware CISCO