AUGUST 2019

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

REMOTE SUPPORT

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. Use a DNS Security Solution as an added layer of protection.

2. Ever come across an email from someone you know that looks a bit phishy? Give the person a call to verify that they sent the email.

3. If you have many open windows cluttering your PC's screen, simply minimize them all and access your desktop by clicking Windows Key + D.

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

People in the 60s: The government will wire tap your home.
People now: Hey wire tap, can cats eat pancakes?

Hiring a new employee?
Let us know as soon as possible so that we can get their network account, hardware, software licensing, and more setup in advance so that they're ready to rock and roll on their first day!

iPhone Vulnerability: Update to iOS12.4 ASAP

If your iPhone isn't running software version 12.4, you'll want to update as soon as possible. There's a bug that can be exploited without any user interaction via iMessage and the code for the exploit is public. Any cybercriminal with a MacOS device and phone number/iMessage account details can attack and spy on a target...UNLESS the target has updated to software version 12.4 that patches the bug.

You can check to see if your iPhone has been updated or not by accessing Settings>General>Software Update.

Capital One Data Breach

Do you use Capital One? If so, there's a possibility that your personal information was exposed. Capital One was hacked... 140,000 Social Security numbers and 80,000 bank account numbers were compromised. The breach occurred back in March and was only detected recently.

While Capital One says that it will notify those affected, it never hurts to monitor accounts for suspicious activity and freeze your credit until it's needed (i.e. if you need to apply for a loan).

Know How to Identify a Spoofed Site?

There's been an increasing number of fake Wal-Mart sites discovered to be stealing people's credit card numbers and personal information. In addition, a fake Office 365 site has been tricking people into downloading malicious browser updates and software. You should always avoid installing any "updates" from browser pop-ups, but it can be difficult to tell if a site is fake (spoofed).

A few ways to tell if a site is a fake include:
1. The URL bar notes "HTTP" and "Unsecure" when the website is requesting you to enter personal/billing information
2. The site's address is misspelled (i.e. Amazonn.com)
3. There are spelling/grammar mistakes on the site

*If you aren't sure if you're on a legitimate page and don't want to risk handing over your personal or card information to a cybercriminal, reach out to the DigeTekS team for verification.

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