MARCH 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

REMOTE SUPPORT

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. Removing/storing old unused files elsewhere can help improve the performance of your machine.

2. If you have too many windows open that are cluttering your screen, press Ctrl + D to minimize all windows and jump straight to your desktop.

3. Are you frustrated with unwanted programs initiating every time you restart your PC? Disable them in the "startup" tab of task manager.

4. Do you often have the need to share sensitive information (i.e. patient info)? Opt for a hosted email encryption service!

2/5
I... CAN'T... GET... IT... OFF!!
DUDE, THAT'S BECAUSE YOUR CAPS LOCK IS ON.
SCOTT HILBURN
©2016 Scott Hilburn/Distributed by Universal Uclick

The luck of the Irish won't mitigate risk of a hack and loss of your files, personal information, and/or financial information. Opt for DigeTekS cybersecurity training, a hosted desktop AV solution, and routine backups to cover some basic security bases and defend against cybercriminals!

Update Your Chrome Browser

Regardless if you use Mac or PC, be sure that your Chrome browser is running the latest update. The NSA recently alerted the public of some critical and nasty security issues that could allow a hacker to easily take full control if Chrome isn't patched. Ensure that you're running the latest version: 1) Click the 3 vertical dots icon in the top right corner of Chrome, 2) Click "Settings" and 3) Click "About Chrome" at the bottom of the left menu.

A patched machine is a protected machine. Always update your devices and programs as updates become available.

Beware of Phishing

Always always ALWAYS be cautious when links and attachments are received in emails or text, regardless if they appear to come from a trusted site or person. Hackers can impersonate your boss, your coworker, or a vendor by using a correct-looking email address, professional verbage, email signatures, and more in order to get you to blindly click away.

Do you know how to identify fake emails intended to trick you into sharing personal info?
1. Check the email address of the sender
2. Hover over (but don't click) links to see where they will take you on the web
3. Does the email contain spelling/grammar mistakes?
4. Always verify odd or unsolicited requests (If the sender's email address is correct, their email account may have been compromised and under hacker control.)

Is Your Router Up To Date?

When was the last time you updated the firmware on your router? If you can't remember, log into your router's admin page and check for any updates. Among the router brands, Netgear recently patched critical vulnerabilities in a dozen of their devices. Not ensuring up-to-date router firmware could allow even the most novice hacker to access your network and any devices attached.

Ring Devices

If a Ring device (i.e. doorbell) is connected to your network, be sure to setup 2-Factor Authentication (2FA) for a layer of security (and privacy). Even if you have 2FA setup for an account, your password for the account should never be the same password as another account's or have ever been used before. Every account's password should be new and unique.

Do you know what type of sites you shouldn't visit on your work computer?

Do you know your company's Internet Acceptable Use Policy (IAUP)? Your company may or may not have measures in place to monitor/restrict access to sites pertaining to social media, adult media, torrent downloading, and more.

If you need access to a restricted site, please review with your manager for access.

DigeTekS Is Partnered With: SEP CITRIX MICRO FOCUS Microsoft SUSE WatchGuard McAfee