OCTOBER 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

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. Always a trick, never a treat..
Never click on pop-ups that claim you have won a prize. The only "prize" you will win by clicking on the pop-up is a big box of regret as your PC and data within is infected by malware.

2. Don't click on links or attachments in unsolicited/suspicious emails. Always verify odd requests or attachments.

3. Having issues loading pages? Depending on the browser you're using and what kind of pages you have loaded, having too many pages/tabs open can be the simple culprit. Slow internet speeds or too many devices connected to your network can also be the issue.

BoOoO! Do you know what's scarier than a ghost?

Not being prepared in the instance you lose your data to cyber criminals! October is Cybersecurity Awareness Month. Do you where your business' defenses stand?

New Stealthy Malware: Nodersok/Divergent

Developing malware (dubbed Nodersok/Divergent) is currently slipping past Windows Defender. The majority of targets are average consumers in the US and Europe. Microsoft advises that users keep an eye out for unrecognized files and avoid running HTML application (HTA) files.

Worldwide Unprotected PACS Exposed Millions of Records

590 unprotected PACS (Picture Archiving and Communication System) servers around the world were accessible online and exposed over 24 million patient records and 730 million images. 187 servers in the U.S. were unprotected by passwords or basic security precautions. Record details include first/last name, DOB, scope and imaging of procedure, and more. The highest number of unprotected PACS and exposed data sets was in the U.S. on specific servers. As of right now, those specific servers have not been disclosed publicly.

More Exposed Data: DoorDash & Words With Friends

Names, email addresses, delivery addresses, phone numbers, and hashed passwords of DoorDash users who joined the service on or before April 5, 2018 have been exposed. Names, email addresses, login IDs, hashed passwords, and more from Words With Friends accounts setup before September 2nd have also been exposed.
If you have an account with either DoorDash or the game Words With Friends, you should change your password and make sure the password isn't being used with the same login email on any other site.

Random Spam Appointments on Your Calendar?

Ever come across an odd/phishy appointment on your calendar that you didn't create? Some calendar application default to automatically accept appointments from whoever, including cybercriminals trying to get you to access a link... Don't click any links or respond to the appointment --- simply delete the appointment and modify your calendar settings to only accept appointments you approve.

Do you know how many characters, lowercase letters, uppercase letters, numbers, and special characters you need to use when creating passwords to access company information?

Do you know your company's Password Complexity Policy? If you're trying to create a new password and the system isn't taking it, you may need to add more characters, a special character, a number, and/or upper-case letter. In general, it's always a good idea to employ all of the above to create a strong and secure password..

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