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.
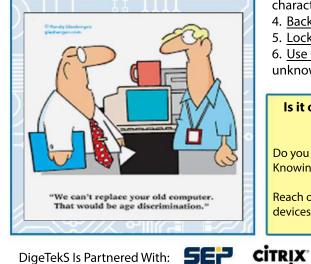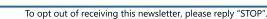
PC Tips & Tricks:

1. Use a strong password (combination of upper and lowercase letters, numbers, and special characters) for each account you may have. Never reuse passwords.

2. Whether it's to the cloud or an external drive, back up your data on a regular basis. This will protect your information from being lost in a disaster, accidentally deleted, or held for ransom by hackers!

3. From Facebook accounts to email accounts, use Multi Factor Authentication (MFA) for each account you can in order to layer and increase protection against cybercriminals trying to access your accounts.

"We can't replace your old computer. That would be age discrimination."

Regardless if a technician is on site, don't hesitate to submit a ticket if you have an issue/work request. You can call the help desk line, reach out to us through our remote support link on our website, or submit a ticket via email to ensure ticket logging and routing.

Data Leak: First American Financial Corp.

Have you used lending provider First American Financial Corp? Do you use an identity theft protection service?

Hundreds of millions of documents related to mortgage deals going back to 2003 (i.e bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers license images) were available without authentication to anyone with a Web browser since 2003...

Be Weary of CrySIS (Dharma Ransomware)

CrySIS (Dharma ransomware) is increasing efforts to target businesses. The ransomware is often distributed as malicious email attachments and installation files disguised as legitimate software, but can also infect systems by exploiting leaked or weak RDP credentials.
How do you protect your systems against ransomware?

Do You Reuse Passwords?

Using the same password for multiple accounts can make it easy to remember how to access your many accounts, but it can also make it easy for cybercriminals to access your accounts, too!

Ex: If a site (such as Facebook) gets hacked and readable credentials are stolen, the hackers will then sell the various stolen creds. Whoever buys the email and password combinations will likely try to access as many accounts as possible using those credentials. Hopefully you didn't use that same login info for another account...

Top 6 Device Security Tips

1. Patch and Patch Often: Stay up to date with software and operating system updates.
2. Always Use Protection: Employ a firewall and use a software that scans your files for threats and updates regularly.
3. Use Strong & Unique Passwords: Use passwords with letters, numbers, and special characters; Never reuse passwords or use the same password or multiple accounts.
4. Backup Data Often: Backup and store a copy of your device's data offline.
5. Lock Your Doors: Always lock your device if not directly in front of it.
6. Use Caution With Unsolicited Emails: Be weary of attachments and links from unknown senders.

Is it okay if you plug your personal electronics (phone, iPod, camera, etc.) into your work computer?

Do you know your company's Acceptable Use Policy (AUP) for hardware and software? Knowing your company's AUP can help keep you and your information and systems protected.

Reach out to your manager for a list of guidelines you should adhere to when using company devices and resources.

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