DigeTekS LLC
di.ge.ra.ti
persons well versed in computer use and technology

IT Consulting	Managed Services	Network Security	Hosted Services

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.

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 Multi Factor Authentication (MFA) on all accounts to increase protection against cybercriminals trying to access your account(s).

2. Always update your devices when an update is available. While some updates may contain new features that aren't necessarily a need-to-have, others may contain fixes for critical software vulnerabilities that hackers could exploit.

3. Use a hosted email quarantine solution to help cut back on the amount of spam you may receive and most importantly reduce risk of infection due to malicious links and attachments within phishing emails.

Congratulations 100,000th Visitor!

You won a free iPad!

Just fill out this small survey and we'll give you your prize!

Social Security Number

System32 Comics

Is Your Company A Sitting Duck For Cybercriminals?

Ransomware Attacks Have Doubled This Year
What measures do you have in place to protect your data from cybercriminals? Is your company a sitting duck? A recent McAfee report notes that ransomware attacks have doubled this year and there's been an increase in brute-force attacks on RDP and SMB...

State Farm Data Breach
State Farm accounts were compromised by cybercriminals using a list of credentials (most likely obtained from another site's breach). While no sensitive personal information was viewable, State Farm has reset the passwords of all users whose accounts were compromised.

If you use the same email and password combination for multiple sites and one of those sites is breached, there's a strong chance that your other accounts using the same credentials will be accessed by cybercriminals in the future... Never recycle passwords or use the same credentials for multiple sites!

Scam Alert: Fake IRS Emails
Cybercriminals are sending fake tax related emails with one-time passwords that are used to access malicious files. If you receive an email claiming to be from the IRS, ignore/report as spam. The IRS will never contact you by email. Links and attachments in emails should be treated with caution, even if the sender appears to be a trusted source.

Spoofed Site Alert: Fake NordVPN Website
A fake NordVPN website has been tricking people into downloading a banking Trojan. The website looks practically identical to the legitimate site. If you are needing to download NordVPN, verify that the core part of the URL address is nothing other than "nordvpn.com" before you initiate any downloads!

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.