NOVEMBER 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!

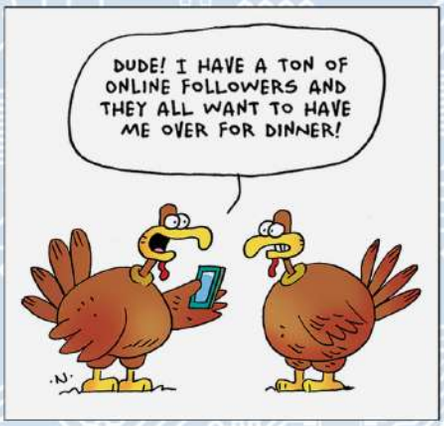
You can call our help desk suport line, reach out to us through our remote support link on our website, or send us an email at supportrequest@digeteks.com.

PC Tips & Tricks:

1. Always lock your devices when you're not directly using them.

2. Do you work and browse the web using free public WiFi (i.e @ Starbucks)? Consider opting for a VPN (Virtual Private Network) service to protect your connections and any information you submit to pages.

3. If a browser window randomly pops up on your screen while browsing telling you that you have a virus, no need to be alarmed. Simply close the window using Alt + F4 on the window. These types of pop-ups are common and do not actually indicate an infection. Never click on links within the pop-up window to avoid risk of actual infection.



For a lot of us, this month kicks off the holiday shopping season. Be weary when shopping online deals and submitting your personal and billing information. Always pay for orders using a credit card and monitor your statement at the end of each month for suspicious charges.

As First Northern Bank of Wyoming's trusted IT partner for over 8 years, we're pleased to announce that our hard work and dedication has facilitated a FIRST PLACE achievement in this year's Cybersecurity Competition for Small Business.

BlueKeep Windows Flaw: Exploitation Now Active

Back in May, a critical zero-day RDP vulnerability affecting older Windows systems was discovered and Microsoft quickly released a patch. The flaw (dubbed BlueKeep) is now actively being used to mine cryptocurrency, but has much greater and disastrous WannaCry worm-like potential. Are your systems patched and protected?

Amazon Alexa & Google Home Security Risks

Security researchers were able to develop Amazon Alexa and Google Home hosted apps that could spy on user conversations and even phish for passwords. The apps passed all of Google and Amazon's security vetting processes... In addition, researchers have now found that cheap lasers can be used to trick the voice assistants into performing known commands (i.e. unlocking or opening doors). You should probably move your voice assistants away from any windows... or remove them from your home altogether.

Adobe Creative Cloud User Data Exposed

An unprotected database exposed email addresses and non-sensitive account information of 7.5 million Adobe Creative Cloud Users. While no passwords or payment info was exposed, the emails that were exposed could soon be targeted by phishing campaigns. How strong are your email security and anti-spam defenses?

Do you know what qualifies as Personally Identifiable Information (PII)?

PII is ANY information that can identify a living individual (such as full name, Social Security number, driver's license number, etc.) and data privacy laws govern the handling of PII. Be sure that you know how to remain PII-compliant in your location and industry!

Review with your manager if you have any questions or concerns.

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