



IT Consulting | Managed Services | Network Security | Hosted Services

**Phone Support:**  
(855) 536-5052 x1

**Email Support:**  
supportrequest@digetek.com

**Remote Support:**  
www.digetek.com



We hope everyone will enjoy Memorial Day on Monday, May 25<sup>th</sup>. Although our office will be closed to observe the holiday, we will be on call and ready to respond to urgent tickets. Please email supportrequest@digetek.com or call our office at (855) 536-5052 to create a ticket.

**Concerns about using Zoom?**

Zoom and other virtual meeting sites have become a necessity for many businesses to continue operating remotely. Zoom's daily usage rates have skyrocketed in the last month despite some very serious security concerns recently. Reports of compromised security include attacks known as zoombombing; Zoom users names and passwords are for sale or displayed on the dark web. Encryption that isn't truly secure, and concerns of servers based in China have been raised as major concerns. Because of these security concerns, Google and the entire US Military banned the use of Zoom from all employee computers.

Although Zoom released an update this week to address known compromises, DigeTekS can provide a multitude of secure platforms for your employees to safely communicate as group. Please feel free to reach out to anyone on your IT team for more information!

**How to work productively and securely from home**

Working remotely can sometimes be challenging. A wireless keyboard and mouse, a laptop stand, noise cancelling headphones, and an additional monitor are all items that can help improve concentration and productivity. Additionally, there are distractions that can make focusing difficult. Having a dedicated workspace and the necessary equipment are all things you should discuss with your supervisor to make sure you have the tools you need to be as effective as you would be in the office.

Ensuring you are working securely from home is also important. Running updates for your antivirus, PC, and all applications can help keep your and your company's data secure. The most effective hacks usually take advantage of known security flaws that you could have easily protected yourself from. Knowing what your company's acceptable use and/or security policy expectations are for you when working on the computer systems can usually help identify the right actions to help keep your business secure. Lastly using multi-factor authentication and an encrypted password manger will add an extra layer of protection. Working with all or some of the above items will help keep your company from being another statistic in the headlines we hear about every day in the news.

**Beware of Coronavirus Spam and Phishing Emails**

Are Economic Stimulus check or Coronavirus related spam and phishing emails slipping past your email's defenses? Phishing, which is the act of tricking you into providing data to an unknown party, is the most common method used by hackers to compromise your data and personal information. By providing real information to a fake link or attachment click, your information or machine could be compromised. Also, never login with your Office365 or Network credentials if a link or document is received from an email; rather contact your manager to ask about this email. Consider opting for a hosted anti-spam filter and/or quarantine to beef up your defenses.

DigeTekS can help! We offer both services to help you protect your information.

**Are you up to date with your cybersecurity training?**

Do you know your company's policies for acceptable email usage? Do you know what items to look for in your email that might compromise you or your workstation?

Ask anyone on your friendly IT team for a refresher of your cybersecurity training before it is too late. Keeping up to date on your cybersecurity training can make the difference between a secure workstation and an infected one.

**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@digetek.com.**

**PC Tips & Tricks:**

1. Always use different and strong passwords for each account. Never reuse passwords across accounts. A strong password should include a combination of upper and lowercase letters, numbers, and special characters. The longer the better.
2. It's never a bad time to do a little PC spring cleaning! Remove or store unused files elsewhere can improve the performance of your machine.
3. From Facebook accounts to email, use Multi Factor Authentication (MFA) to increase protection against cybercriminals trying to access your accounts.

