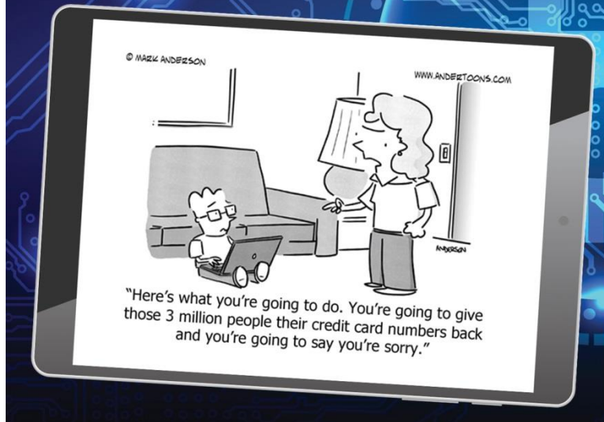
Funny Business



OCTOBER 2018
CYBERSECURITY AWARENESS MONTH

1 • International Coffee Day
3 • Techie's Day
16 • Steve Jobs Day
17 • Spreadsheet Day
31 • Halloween

5K TechnicalServices
ENHANCING PRODUCTIVITY, ONE CUSTOMER AT A TIME
ASSESS | ON-BOARD | MANAGE | PROTECT | OPTIMIZE

5K Technical Services
100 Allentown Parkway Ste 104
Allen, TX 75002
(469)656-3159
info@5ktech.com
www.5ktech.com

October is...
CYBERSECURITY AWARENESS MONTH

5K Technical Services Presents:
Tech Times

Did You Know That October Is National Cybersecurity Awareness Month?

Online security is something that should get everyone's attention. Threats exist all around us: ransomware, viruses, spyware, social engineering attacks and more. There's so much you need to know to keep your personal and business information safe.

But... where do you start?
As trusted cybersecurity professionals, we want to help you get educated and stay informed. That's why during National Cybersecurity Awareness Month our goal is to give you all the information you need to stay secure. How can we help? We'll be sharing valuable and timely information on cybersecurity in blogs, in our newsletter, and on all of your favorite social media sites.

What should you do?
You can also give us a call for personalized solutions by subscribing to our exclusive mailing list. Being cybersecurity aware means that you understand what the threats are and take precautions to prevent them.

Here are some important reminders:

- Never give out your password. Don't share it over the phone either. You never know who's listening.
- Don't click on links that are sent to you via unsolicited emails or from someone you don't know.
- Use complex passwords that are difficult to guess and use different ones for different programs and computer devices.
- Don't reveal your personal, business or financial information in emails.
- Don't respond to email solicitations.
- Keep software, browsers and operating systems up to date, so they stay free of vulnerabilities.
- Encrypt your files to ensure unauthorized people can't access them.
- Be careful when using public Wi-Fi networks – don't conduct sensitive activities like banking or shopping with credit cards on public Wi-Fi.
- Remember your physical surroundings and don't leave your computer devices unattended in public or easy-to-access areas.
- Only use websites that begin with "https://" when visiting online shopping, banking or other sites where you will be entering your private information.
- Keep your online presence private. Don't publish your email address online in social network sites.

What to do if you become a victim of cybercrime?

- Report it to the appropriate people in your organization, including your network administrator.
- If you think your financial account was compromised, contact your financial institution immediately and close your account.
- Watch for any unauthorized charges in your bank or credit card accounts.

We hope this helps. Remember, we'll be posting timely cybersecurity information for you in our Bogs, newsletters and more.

New Technology:

Colorado Timberline Taken Down by Ransomware and What That Means for You

According to Statista, there were 184 million ransomware attacks in 2017 and the average ransomware demand is over $1,000. Individuals, organizations, and companies have fallen victim to these attacks. Most people recognize the fact that ransomware is a danger, but they may not realize that it can actually destroy their company. The recent closure of Colorado Timberline after a ransomware attack is a solemn reminder of the seriousness of the dangers of ransomware.

What Happened to Colorado Timberline?
Colorado Timberline, a printing company in Denver, was forced to cease operations for an unspecified amount of time after a severe cyber-attack. A statement on their website dated September 12th stated that they had been the victim of several recent cyber-attacks, but the last – a ransomware attack – was something they would not be able to immediately recover from.

What Happened in the Ransomware Attack?
The data locker ransomware attack took place on the evening of August 14. The ransomware accessed their database server and encrypted the files it contained. The issue that Colorado Timberline ran into, according to an explanatory post for their customers via their Facebook page, was that the hackers insisted that physical access to their files was necessary in order to obtain the encryption key even if the ransom were paid.

Colorado Timberline explained that it was not a matter of paying the ransom, but granting the hackers further access to their data was their greatest concern. Instead, they opted to make use of their data backups to restore the system and had their IT staff doing their best to extract as much data as possible from the encrypted database server.

About Colorado Timberline
Colorado Timberline's LinkedIn Page indicates that they had between 200 and 500 employees and that they had been in business for five years. They specialized in printing, including vinyl, apparel, banners, glass etching, and large format applications. In 2017 they were acquired by two out-of-state companies and their owner left in May. What impact that may have had on the decision to cease operations is not known.

How Data Locker Ransomware Works
Data locker ransomware malware (also known as a crypto ransomware) gains access to a computer, then it begins to search through the file system to find data that would be of value to the victim. It stays hidden as it both searches for this data then encrypts it. Once the encryption is complete, the malware alerts the user with a message announcing that data has been taken hostage and encrypted. It will indicate how the ransom is to be paid (usually in a type of cryptocurrency, ironically) and how long before the decryption key is destroyed, and the data rendered useless.

The first wave of modern ransomware attacks began to take place in 2015, according to "The Evolution of Ransomware" published by Symantec. The history of ransomware, however, can be traced back to 1989 where the first target was healthcare data systems. Now any company with valuable data is a target for attack. And, as with any type of hacking activity, the methods for infecting a computer with ransomware are continually evolving and improving. It is important for every business and organization, small or large, to make sure their cybersecurity systems are powerful enough to protect them and up-to-date against the latest threats.

Do You Know How to Add Email Signatures?

A compromised endpoint gives hackers everything they need to get a foothold in your security network. Once there, they can steal data and potentially hold it for ransom. That's why it's so important for business owners to secure their critical endpoints (including desktops, servers, and laptops). Otherwise, you could be leaving the front door wide open to hackers.

Today's attackers have learned how to bypass traditional antivirus software by using file-less attacks. These types of attacks can hide within sanctioned applications or even within the operating system. Even if you're vigilant about installing antivirus updates and patching, your organization may still be at risk.

What Are Endpoints?
Endpoints in networks are computer hardware items within the TCP/IP connections, which may include desktops, laptops, smartphones, tablet devices, printers, meters, terminals, smartphones and mobile devices, clients, and other forms of hardware.

Endpoint protection (EPP) has evolved to encompass code-based hacking, but the approach is often not adopted as organizations chose to use a legacy solution due to convenience or a lack of sufficient familiarity. Online sources including MSSP report this is common, but improvements in EPP will lead to more mainstream adoption. Meanwhile, current users may find that their existing network and operational variables demand some kind of improvement.

What Should I Know About Current Endpoint Security Risks?
One sign of a demand for improvement is continuing to use an antivirus program operating on a signature base. This form of technology is considered to be too slow to keep up with so-called 'zero day attacks,' or malware programs that are integrated with other coding.

Users should expect potential vulnerability with such programming, and devices that are not updated daily are considered vulnerable to ongoing malware threats. Additionally, signature sets (lists of operational protocol) can become so large that they run into the limit issue, leading legacy vendors to drop them, which creates a demand for new solutions that do not use signatures.

Another potential reason you may need to address your EPP is the increase in 'ransomware' attacks. Ransomware, hacks designed to block user access until funds are provided to the hacker, has become increasingly destructive in the past few years. All it takes is one careless user who clicks on a link in an email, and your entire database could be locked until the ransom is paid.

Demands for improved management of antivirus software and continuing to use on-site antivirus management servers may also be grounds for improving EPP. You should be able to manage your entire antivirus system from your cloud, and if you cannot, you should consider updating and improving your system. Meanwhile, however, you should take care to ensure that any increased internet connectivity involved with a system improvement does not involve increased vulnerability. If you are able to manage your antivirus system from your cloud, but it does not seem to be sufficiently organized or efficient, you may benefit from substantial restructuring. Other practical reasons for investment in End Point Protection integrations or improvements include a developed distrust of your current system. Directly targeting EPP can be more efficient and effective.

If you are still doing regular background scans, or your new machines seem slower than you think they should be, you may want to consider improving your EPP. The newer generations of antiviral protection do not require background scanning. Traditional processes for security may be insufficient in addressing the range of possible endpoint attacks.

Tech Insights:

Want to Learn 3 Cool LinkedIn Tips?

Profile – Viewing – Searching

We get questions from our clients about using LinkedIn all the time. And we get so many that we've been keeping track of some of the most commonly asked ones. We've posted three of them here with detailed answers for you.

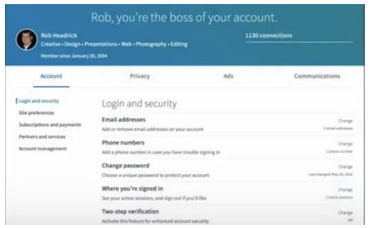
1. "Is There A Way To Change How My Profile Is Viewed?"

Sometimes you want to change the way your profile is viewed. Perhaps you're looking for a new job, or you've just gotten one.

Or, maybe you're working a second job and you don't want your boss to see this. With changes in your business life, you want to keep track of what's important to post on LinkedIn.

Here's how to change or update how people see you on LinkedIn.

Click **Me**; Click **Settings & Privacy**; This is what you'll see…

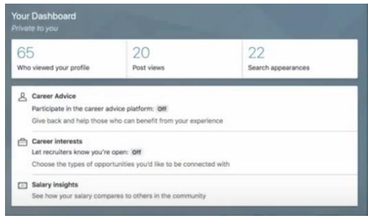


Click the **Privacy Tab**.

LinkedIn will give you half a dozen options to change your privacy settings for changing who can see what information about you.

2. "How Do I View My Post Statistics In LinkedIn?"

If you've ever posted an article or video to LinkedIn, you can see specific demographics about your readers. To see these stats, just like you did above, click on **Me** and **View Profile**. Now, scroll down until you see this Dashboard section. Click on **Post views**.



Next, click on the Posts tab. Now, scroll down to one of your articles. On the lower left click the view counter next to the line graph icon. LinkedIn will provide you details of who viewed your article. The stats are broken down by company, title and location.

3. "How Do I Use Boolean Search Terms In LinkedIn?"

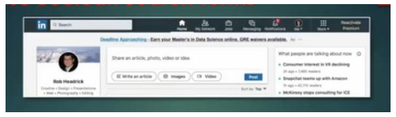
LinkedIn provides powerful search capabilities. It can take a while to efficiently use the power of people search. But it's worth taking the time to learn. LinkedIn gives you the option to use Boolean Search Terms to perform more specific searches. You can do this by adding or eliminating elements to the search parameters.

(Boolean logic is a system of showing relationships between sets by using the words AND, OR, and NOT. The term Boolean comes from the name of the man who invented this system, George Boole.)

Boolean Operators are used to connect and define the relationship between your search terms. When searching electronic databases, you can use Boolean operators to either **narrow** or broaden your **record sets**. The three Boolean operators are AND, OR and NOT.

Here are some examples of Boolean search strings:

- infographics **AND** presentations
- copyediting **OR** copy editor
- Google **NOT** Salesforce



Let's say you wanted to find someone who is an expert in presentation design. You should use this as a key term in your search.

When you do, your search results will come up with anyone who has the words presentation and design in their profile even if the two words are located separately in their LinkedIn profile.

But by adding quotes around "presentation design" LinkedIn will only list those people with the two words together in their profile.

Parenthetical Searches
If you'd like to perform a complex search, you can combine terms and modifiers and use parentheses.

That's it! Three tips you can use to improve your overall skills in LinkedIn.

October Special

October is…

Cybersecurity Awareness Month

5K TechnicalServices
ASSESS | ON-BOARD | MANAGE | PROTECT | OPT | MIZE

Are you 100% confident in your ability to stop a cyber threat?
Book your FREE cybersecurity evaluation.
Free until October 31
Call (469) 656-3159 or email info@5ktech.com and book now.

Quotes of the Month

"The true sign of an uber-successful organization is that they do what's not expected of them."
Nikos Kazantzakis

"Always deliver more than expected."
Larry Page, Co-Founder of Google