BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle

October 2020

Top Tips to Securely Using Social Media

Social media sites, such as Snapchat, Facebook, Twitter, Instagram, and LinkedIn, are amazing resources, allowing you to meet, interact, and share with people around the world. However, with all this power comes risks--not just for you, but your family, friends, and employer. In this newsletter, we cover the key steps to making the most of social media securely and safely.

Posting

Be careful and think before posting. Anything you post will most likely become public at some point, impacting your reputation and future, including where you can go to school or the jobs you can get. If you don't want your family or boss to see it, you probably shouldn't post it. Also, be aware of what others are posting about you. You may have to ask others to remove what they share about you.

Privacy

Almost all social media sites have strong privacy options. Enable them when possible. For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

Marco's Corner

Nearly every week, you hear a news story about a cyber-attack or a rogue virus sweeping through the country or the world. And maybe you're a little bit skeptical. Are these viruses really a problem for you? Why would hackers bother with a small company, such as my own? And are these cyber-attacks really aimed at a business like yours? The answer is a very simple "you bet they do". So, we thought it might be fun to share what Biz-Net services provides and how we keep you safe. For example, in just the last 12 months, we have done the following: stopped viruses from attacking; kept computers and servers safe from those attacks; continue to educate ourselves on all varieties of threats out there; replaced old, outdated firewalls to better protect our clients; monitor your business network 24x7x365. There IS a very present threat to your company, and we are always watching your back. For another layer of protection, we also deliver the best Backup Services (Business Continuity) in the business that acts as fire insurance for your data. If you're not 100% sure you're protected, give us a call today. You can also download our report on ways to protect your business at www.biz-net.com/haunted. Call us today at 775-850-7700 for further information on all the services we provide.

Get More Free Tips, Tools and Services At Our Web Site

www.biz-net.com

(775) 850-7700

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502
www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

Passphrase

Secure your social media account with a long, unique passphrase. A passphrase is a password made up of multiple words, making it easy for you to type and remember, but hard for cyber attackers to guess.

Lock Down Your Account

Even better, enable two-factor authentication on all of your accounts. This adds a one-time code with your password when you need to log in to your account. This is actually very simple and is one of the most powerful ways to secure your account.

Scams

Just like in email, bad guys will attempt to trick or fool you using social media messages. For example, they may try to trick you out of your password or credit card. Be careful what you click on: If a friend sends you what appears to be an odd message or one that does not sound like them, it could be a cyber attacker pretending to be your friend.

Terms of Services

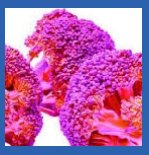
Know the site's terms of service. Anything you post or upload might become the property of the site

Work

If you want to post anything about work, check with your supervisor first to make sure it is okay to publicly share.

Follow these tips to enjoy a much safer online experience. To learn more on how to use social media sites safely, or report unauthorized activity, check your social media site's security page.

Random Interesting Fun Facts



McDonald's wackiest attempt at making their menu more nutritious was to design broccoli that tasted like bubble gum.

Movie trailers originally played after the movie, "trailing" the feature film. The first trailer appeared in 1912.

Scotland has 421 words for "Snow." including "snaw" (snow) and "sneesl" (to begin to rain or snow).

Cats have fewer toes on their back paws. They have five toes on the front, but their back paws only have four toes.

Thanks to 3D printing, NASA can basically "email" tools to astronauts making them ready within hours.

In Switzerland it is illegal to own just 1 guinea pig as they're social animals, and are considered victims of abuse if alone.

Security Issues Increasing With More People Working From Home

According to a recently published report by Malwarebytes, the global pandemic may be behind the recent surge in cyberattacks against businesses of all sizes.

While it wasn't immediately apparent, the pandemic forced businesses around the world to respond quickly to the emerging pandemic. As a result, tens of millions of workers began working from home.

In most cases, the infrastructure to make that possible was put in place very quickly, and as a result, the security surrounding that infrastructure wasn't as robust as it could have, or should have been. Hackers from around the world, always quick to take advantage of such situations, began striking at the new legions of homebound employees, finding easy pickings.

Based on the findings of the Malwarebytes research, nearly a quarter of organizations have found themselves having to pay unexpected costs to address malware infections or data breaches since shelter in place orders were imposed.

The three most common weak links were found to be:

Improperly secured corporate VPNs
Business eMail compromise
Improperly configured security and access controls to cloud-based data
That makes a certain amount of intuitive sense, given that in many cases, those are the kinds of things that would have been hastily rushed into place. It all went so fast, as businesses scrambled to respond to the new realities of the workplace which the pandemic imposed.

Adam Kujawa, one of the researchers responsible for the report, had this to say:

"Threat actors are adapting quickly as the landscape shifts to find new ways to capitalize on the remote workforce. We saw a substantial increase in the use of cloud and collaboration tools, paired with concerns about the security of these tools. This tells us that we need to closely evaluate cybersecurity in relation to these tools, as well as the vulnerabilities of working in dispersed environments, in order to mitigate threats more effectively."

Wise words. If your business has seen a radical change in the way your employees work in recent months, and it probably has, now is the time to conduct a thorough security audit to limit your exposure.

New Features Have Been Added to Office 365

If you're an Office 365 user, you'll be pleased to know that that Word for the web now has two cool new features: Transcribe and support for voice commands.

Currently, the transcription capabilities are somewhat limited, but are still robust enough to be genuinely useful. At present, it only supports transcribing audio into US English.

In order to make use of that feature, you need to be using Microsoft Edge, Chrome, or some other Chrome-based browser. The best part about the new feature is that the actual transcription takes place on the web, so there's no need to download and install a third-party app to handle audio files.

In addition to that, the new transcription feature automatically detects different speakers in recorded conversations and transcribes them accordingly, which makes it easier to follow the flow of conversation in a transcript generated in Word.

Dan Parish, the company's Manager of Natural User Interface and Incubation, had this to say about the new feature:

"Your transcript will appear alongside the Word document, along with the recording, which enables you to leverage your transcript to create great content in the way that works best for you."

Although these may change at any time, currently, Microsoft has placed the following parameters on use of the new feature:

Users are limited to five hours of transcription time per month
Uploaded audio files must be in one of the following formats:
.mp3
.wav
.mp4
.m4a
Uploaded files may not exceed 200 mb in size.
Even given these restrictions, this is an awesome new addition.

The second enhancement to talk about here are the voice commands.

Dan Parish had a few words to say on that topic as well:

"We've been adding voice commands to Dictate so that you can break away from the keyboard. Whether on the desktop or mobile (or transitioning between devices), you can stay in the flow and focus on your message by using dictation with voice commands to add, format, edit, and organize your text."

Microsoft has a full list of Dictate commands the software will accept, and the system even understands a variety of symbols, which is super convenient.

Kudos to Microsoft for the amazing addition. It's absolutely fantastic and will make your life easier.