PenTeleData

THE NetworkGuy

JUNE 2021 \ VOLUME 2 \ ISSUE 6

What's Inside...

Productivity App:

Google Calendar

Google Calendar is free, works across devices, and works well for both individuals and teams. It lets you manage multiple calendars using multiple views and color-coding; set reminders; and more. Your events are stored online, so you won't lose your schedule, even if you lose your phone.

The Network Guy Quiz Challenge

PenTeleData is giving one lucky winner a $150 Amazon Gift Card. Just visit **www.ptd.net/quiz-challenge** by **June 30, 2021** to answer the question below. We will select a winner at random from all correct entries. **Good Luck!**

What is the most used social media platform among the Gen Z population?

Learn from The Network Guy

I received an email that appeared to be from my bank, but the letter "O" in the link to their website looked more like a zero. Is it still safe to click the link to visit my bank's site?

The Network Guy:

That's a good question! Don't click the link. Hackers use visually similar characters to deceive people in online phishing schemes. The use of custom fonts to implement a substitution cipher that makes the source code of the phishing page appear as plaintext. The attack is a form of spoofing. Spoofed hyperlinks and websites are a red flag for a potential attempt to steal personal information.

CISA, part of the U.S. Department of Homeland Security, recommends three steps to avoid falling victim to the scheme:

- Avoid clicking on links and instead type the web address into an Internet browser.
- Keep web browsers up-to-date because older versions have fewer protections in place.
- Hover over links before clicking on them to see the true destination. If the web address the link directs to is unfamiliar, it might be an attempt to deceive you.

PenTeleData
JUNE 2021

THE NetworkGuy

"There is a superhero in all of us. We just need the courage to put on the cape."

– Superman

Social Media Statistics & Facts

If you've ever wondered about the effects of social media, here is a collection of social media statistics and facts from 2020:

Worldwide there are 2.77 billion social media users, up from 2.46 billion in 2017.

Facebook currently has 2.27 billion users.

Twitter currently has 336 million monthly active users.

Instagram has 1 billion users.

LinkedIn has 500 million users.

People spend an average of 2 hours and 15 minutes per day on social media networks.

81% of marketers found that increased traffic occurred with as little as 6 hours per week invested in social media marketing.

Infographics are liked and shared on social media 3X more than any other type of content.

The average attention span in 2000 was 12 seconds. In 2020, the average attention span was just 8 seconds. That is less than the 9 second attention span of an average goldfish.

Business to Business audiences largely prefer LinkedIn (82%), Twitter (66%), YouTube (64%), Facebook (41%), and SlideShare (38%) as their preferred social media platforms.

71% of consumers who have had a good social media service experience with a brand are likely to recommend it to others.

Facebook shows the most powerful social media ecommerce statistics, sending a massive 60% of all ecommerce referrals for last year.

Top brands on Instagram are seeing a per-follower engagement rate of 4.21%, which is 58 times higher than on Facebook and 120 times higher than on Twitter.

Facebook Messenger and WhatsApp are the top messaging services, with over 50% of internet users using one or the other.

Snapchat usage is highest amongst the Gen Z population (38% regularly use it).

Over 400 million people use Instagram Stories each month.

Over 2 billion messages are exchanged between brands and users each month, with 45.8% of people saying they would rather contact a business through messaging than email.

Over 90% of marketers who employ an influencer marketing strategy in social media believe it is successful.

Top Internet Safety Rules for Everyone

> Keep your confidential data offline. Cybercriminals cannot access your information if it's nowhere to be found online. Storing important documents offline is the best way to protect them.

> Some data - such as your Social Security Number - should never go online. However, when you still have to share it, be sure to send as an email attachment. Also, feel free to encrypt the file before sending.

> Check a website's reliability. Only signing up to reliable websites is best practice. But how do you know if a website is reliable? First, look at the address line: it should have a little padlock at the beginning - this means the connection is encrypted. Second, review the look and feel of a website. Be sure that the page looks neat and is free from mistakes, grammar is consistent, and ads don't obscure the main content.

> Use strong passwords, with a mixture of upper- and lower-case letters, numbers, and special characters.

> Use two-factor authentication. 2FA or two-factor authentication is used to provide your account with additional protection. When you sign into your account with 2FA, you must not only enter the correct password, but also an additional code generated earlier or sent to your device. If someone just gets a password for your account, they will not be able to access your profile without entering this additional code.

> Avoid suspicious online links and email attachments. These include spam emails, click bait, online quizzes, tabloid headers, free offers, and unsolicited ads.

> When visiting a website, make sure both text and accompanying links are on the same subject. If you click a link to read more about polar bears and instead of seeing the Arctic, you get a 'success story' about a celebrity who lost weight or gave up smoking overnight, then it's better to quickly leave the page.

> Keep your computer software up-to-date. It's important you use the latest versions of your operating systems and apps. Especially if these apps contain your payment, health, or other sensitive info. Developers are constantly working to make products safe, monitoring the latest threats and rolling out security patches in case of vulnerabilities.

> Beware of free downloads. If you decide to go for a free solution, make sure it has a reliable reputation: research the name of the service or software and you will probably find some feedback on how it works.

> Avoid accessing your bank accounts or making purchases via public Wi-Fi. If you need to use this, use VPN software to get some protection for the data you send over the unsecured network. If the transaction can wait, it's best to wait until you can use a private network.

> It's easy to get lost in the flood of online information we're exposed to everyday. If you find something questionable, do your own research to find out the truth or - at least - make up your own mind on a matter. Reliable websites should have references to the original information source.

> Secure your Internet connection with VPN. A VPN makes your Internet connection private by changing your IP address. It also hides the sensitive data you send over, including bank details when you're shopping online and other private information that can be compromised.

> Use cybersecurity software.

> If you have children or elderly relatives, be sure they understand a digital footprint. Talk about what others may learn about you from these search results and how we leave a digital footprint on the Internet, even when that's not our intension.

> Create family rules for shared content. Clearly define for the whole family what content should and shouldn't be shared online. Photos and personal information such as your home address and phone number should be among the first on the list.

> Help your child detect phishing. Explain to your child how to avoid messages, links, or emails from strangers asking for account information or featuring an attachment.

> Teach your child to create strong passwords. You can tell your child that an effective password must contain different characters and warn that it should not be shared with anyone.

> Encourage positive communication online. Explain to your child the importance of behaving politely online and to treat others the way you want to be treated. Just like in the physical, offline world.

(Some information contained in this list is borrowed from https://clario.co/blog/top-internet-safety-rules/)