PenTeleData

THE NetworkGuy

OCTOBER 2021 \ VOLUME 2 \ ISSUE 10

What's Inside...

Learn from The Network Guy

What is a digital footprint and why should I care?

The Network Guy:

A digital footprint is anything about you or put out by you online. It's a trail of data you create every time you use the Internet. It's an impression of the websites you visit, your card purchases, comments and "likes" on social media, smartphone usage, Skype calls, app usage, email records, pictures, even what devices you use. It's a growing picture of who each of us is, probably more public than most assume.

Why does it matter? How is your digital footprint used? The Internet is a public resource. These records help companies target content to specific markets and consumers. Your digital footprint is used to obtain information about you, such as demographics, religion, political affiliations, and interests. Information is also gathered by using cookies, which are small files that websites store on your computer after your first visit to their site that track user activity. Cookies also allow you to hold items in your shopping card, store preferences or login information and make personalized suggestions based on your location or interests. This helps advertisers target you with customized ads. (That's why if you view a product online, you will later see ads for similar items.) Your digital footprint can also be used by employers, both current and prospective. In the wrong hands, it can also facilitate identity theft. If your digital imprint is done right, it can provide a great first impression of you, especially to employers. If hiring managers are impressed by the content they find, such as thought-provoking commentary or stand-out industry articles, they may be more likely to reach out to you for an interview.

It's impossible to remove all traces of yourself from the Internet, but luckily, there are some steps each of us can take to manage our digital footprints.

- Google yourself. Be aware of what others see about you.
- Protect your personal data. Don't disclose your address, phone number, passwords, or bank card numbers. Consider using nicknames instead of your real name.
- Never share your usernames and passwords.
- Limit how you post and respond to pictures. Any photo you share could be used again in the future. Sometimes a few minutes of humor isn't worth a lifetime of potential humiliation. Sharing questionable images also becomes part of your digital footprint.
- Think before you post. A temporary emotion becomes permanent on the Internet. Pause before you post or react to anything online.
- Review and understand privacy policies and Terms of Service for websites you visit. That way, you'll know how they use your information and habits.
- Deactivate social media accounts that you don't use (and be cautious of the activity on the ones you do use).
- Deactivate and delete old email accounts.
- Delete your search result history.
- Ask your telephone provider to make your number unlisted.
- Unsubscribe from email and text alerts.
- Be cautious about what you publish and where you share.
- Review your privacy settings.

The Network Guy Quiz Challenge

PenTeleData is giving one lucky winner a $150 Amazon Gift Card. Just visit **www.ptd.net/quiz-challenge** by **October 31, 2021** to answer the question below. We will select a winner at random from all correct entries. **Good Luck!**

What is most important when choosing a password?

PenTeleData
OCTOBER 2021

THE NetworkGuy

"It's not who I am underneath, but what I do that defines me."

– Batman

Better Broadband Means More Wi-Fi

Wi-Fi is a regular part of broadband at home and plays an ever-growing role outside the home in transit, outdoor spaces, and smart cities applications.

53%
Share of US Internet traffic delivered over Wi-Fi [57% projected for 2022]

500B
Internet-enabled devices expected by 2030

$500B
Amount Wi-Fi contributes annually to the economy

22M
Cable Wi-Fi hotspots across the U.S.

(Source: https://www.ncta.com/broadband-facts)

Password Security

Whether you're banking or shopping online, doing research or social networking, you need account passwords. Unfortunately, the more details you share, the easier it is for cybercriminals to use your information. One way to help keep your personal details safe is to choose strong passwords.

Here's how:

Do not use personal information in your password.
Using personal information as part of or as your entire password is a security risk. It is very easy for someone to guess things like your last name, pet's name, birthdates of family members, phone number, and other similar details.

Avoid using real words as your password.
There are hundreds of tools available to help attackers guess your password.

Be sure that your password is secure.
You can make a password more secure by using a combination of characters. Use some upper-case letters along with lowercase letters, numbers, and even special characters such as '%' or '@'. (Example: C@mpuT3r).

Choose longer passwords.
While it stands to believe that any password created would be secure enough and nobody should be able to gain access to it, shorter passwords are easier to remember and to decode. Though longer passwords can be harder or more cumbersome to remember for you, it will also be harder for anybody else to guess. It's even a good idea to consider passphrases instead of just one word.

Don't recycle your passwords.
Though very tempting, reusing passwords is a security risk to your account and/or personal information.

Use caution when saving your password.
Most current web browsers have features to save your password for later visits. If you are not the only person who uses the computer, you may not want to save your password.

Change your passwords often.
For maximum security you should change your password(s) often.

Use Two-Factor Authentication.
Two-Factor Authentication, or 2FA as it's commonly abbreviated, adds an extra step to your basic log-in procedure. The password is your single factor of authentication. Using the second factor makes your account more secure. This may be a PIN, a password, a fingerprint or another identifying factor.