4-6 Perry Street
PO Box 1662
Wapakoneta, OH 45895

Located in historic downtown Wapakoneta, Ohio, FNGi has been instrumental in developing and supporting Internet Networks across the U.S. since 1993. The FNGi team can assist you with all phases of your Internet Network from initial planning through long-term support.

www.network1.net
800.578.6381

FOCUS Newsletter

In this edition we welcome spring into our lives. We give you an update on our COVID-19 response, then we deep dive into password security. Our President, Stephen Walter provides us a look at password hygiene and then we examine all the current web browser's ability to keep your passwords convenient and safe.

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS April — June 2020

In This Issue

COVID-19 Impact

The COVID-19 coronavirus has presented challenges for all of us as business, communications professionals, and Network Services providers. Together we are meeting those challenges.

To date, no First Network Group employee has tested positive for the virus. We hope the same is true for your companies and for your families. As part of executing our "crash plan", our employees are now working from their homes. It has been our intent that these changes should be invisible to you and your customers - and to date, we have been able to accomplish that.

Our business and yours have been built on crisis response and in a sense this is just another crisis, albeit a global one and a long one. Our practices have changed; our business model and our core principles have not. We at First Network Group are here to provide you and your customers with a superior level of service and support.

Please let us know if you need anything additional from any of our teams. Our Call Center provides support for Triple Play, Billing and Law Enforcement Exigent Requests for several of our customers as well as our Premier Internet Support. Let us help you through this crisis - we are built to help! We extend our best wishes for your continued health and we all look forward to the resolution of this current crisis.

FNGi	www.network1.net
IT Services	1-800-578-6381 Option 1 it@network1.net 24 hours, 7 days a week
Product Development including the DHCPatriot	1-800-578-6381 Option 3 dhcpatriot@network1.net 24 hours, 7 days a week
Tech & Call Center Services	1-800-578-6381 Option 6 callcenter@network1.net 24 hours, 7 days a week
Randy Carpenter Executive Vice President	419-739-1212 (Direct) rcarpen@network1.net
Darren Ankney VP of Product Development	419-739-1233 (Direct) dankney@network1.net
Cory Lykins VP of Tech Services	419-739-1237 (Direct) coryl@network1.net

From the Desk of *"The Network Guy"*

Data breaches have become so frequent that they are becoming smaller and smaller news, yet they are a larger and larger threat to you and to your customers. Data breaches can be particularly damaging for the financial and other private data they expose, leading to identity theft. Not necessarily from the initial hack but from the data that is exposed because of poor password hygiene.

According to SELFKEY, "State of the breach December 2019: AT LEAST 7.9 billion records, including credit card numbers, home addresses, phone numbers and other highly sensitive information, have been exposed through data breaches in 2019." And, "Experian has published statistics showing that 31% of data breach victims later have their identity stolen."

How does this happen, the identity theft, if the breach doesn't contain credit card numbers or other sensitive information? Poor password hygiene.

For example, Jon Doe may not have lost any critical personal information in the breach of the data at Microsoft in 2019, but it may have exposed a username and password that he reuses across many accounts. Usernames and passwords harvested in the breach are sold on the black market to Black Hat hackers who exercise them at different sites until they find a match. In our example, while the hackers didn't get a social security or credit card number from the Microsoft breach, they did from First National Financial where Jon used the same username and password.

Human nature is the reason that password maintenance so important. For most of us, it would be difficult to remember dozens of 12 character passwords. By the time we are adults, we have probably memorized a handful of phone numbers, birthdays and addresses, and of course, our Social Security Number. Simple passwords are often created from numbers or phrases we already know. Second, once we memorize a password, it is easy for it to become THE password, the default password we use for every new account. Soon, that username and password combination is everywhere, from our email account to video streaming or gaming, to shopping and banking.

Given the enormity of dozens or hundreds of accounts, how could anyone hope to keep track of secure passwords that are mixed case, randomized and of sufficient length to be a challenge to hackers? The answer lies in software. Software to create and maintain complex passwords. Some operating systems have password services built in. Others support third party applications for password management.

Apple iOS will generate and store passwords for websites and apps. Stored passwords can be found and managed at Settings -> Website & App Passwords. The actual password screen will show alerts when passwords are reused, making it easy to identify accounts where passwords need to be changed. The current version of MacOS, Catalina, handles this slightly differently. The Keychain Access app can be found with Finder by typing Key in the Finder search bar.

There is a drawback with these tools. While they encourage you to change your passwords, not all websites are written to support the automatic password generation. (I recently visited a major site run by a large multinational corporation where on update, the username field populated with a suggested strong password instead of the password field.)

For more information on password management, see Cory's article "Password Management in Your Browser" in this issue.

Regardless of the ecosystem you use or the password management tools you choose, good password hygiene - complex strong passwords that are unique from account to account - is the first and best line of defense when it comes to controlling your losses from data breaches resulting in identity theft.

Please feel free to share this information with your customers and help them avoid the pitfalls associated with poor password hygiene.

Stephen C. Walter
"The Network Guy"
Founder and President, First Network Group, Inc.

Password Management in Your Browser

Our information is only as secure as our passwords. Cell phones have brought biometrics and two-factor authentication to the forefront of the population when they think about security. But what about your computer's web browser? Let's take a look.

Google Chrome

Chrome is the world's most popular web browser, as such you are probably familiar with it. Google Chrome stores all passwords on your local machine in a heavily encrypted database using the operating system's built-in encryption methodology. If you want to view these passwords within Chrome, you have to confirm your identity to the operating system.

Google also offers the option to synchronize this data to all of your devices with your Google Account. The transmission of this encrypted file is done via an encrypted path.

Strong

- Highest level local encryption
- Passwords are shown one at a time
- Encrypted sync path
- Encrypted cloud storage

Weak

- Weak operating system passwords create easy access
- Weak Google Account passwords create easy access

If you use Google Chrome and allow it to save your passwords, make sure that your computer's login password and Google Account password are very strong and unique from any other password you use.

Mozilla Firefox

Firefox is still a very popular web browser for many to use, and the only browser to not use the same rendering engine that is the basis of Google Chrome. Firefox is unique in a lot of other ways as well, but how does its password handling hold up?

Firefox stores all local passwords in an encrypted database file, however it does not password protect access by default. If you leave your computer accessible, your passwords in Firefox are as well.

Strong

- Highest level local encryption
- Passwords are shown one at a time
- Optional "Master Password"

Weak

- Weak operating system passwords create easy access
- Does not suggest setting a master password by default
- Cloud storage and sync only with optional Firefox account that most people do not have.

If you're using Firefox, make sure that your operating system password is very secure and unique and consider setting a Master Password in Firefox to keep things safe when you leave your device unattended.

Microsoft Edge

You may or may not use Microsoft Edge, but it comes pre-installed with every version of Windows 10. Recently Microsoft has completely reworked Edge from the inside out and the browser is now built on the open source Chromium browser making it very similar to Google Chrome and all other browsers except for Mozilla's Firefox.

Edge (past and present) stores passwords locally using device encryption and allows you to setup an encrypted cloud sync with a Microsoft Account.

Strong

- Highest level local encryption
- Passwords are shown one at a time
- Encrypted sync path
- Encrypted cloud storage

Weak

- Weak operating system passwords create easy access
- Weak Microsoft Account passwords create easy access

Like Google Chrome, if you use Microsoft Edge, make sure that your operating system's login password is secure and unique as well as your Microsoft Account password (if different).

Internet Explorer

Please, stop using Internet Explorer completely.

Internet Explorer version 10 and below have ceased to receive security updates or support from Microsoft on January 1st, 2020. Internet Explorer 11 (the last ever version), will be supported on Windows 10 for the near future, but not on other operating systems.

If you MUST use Internet Explorer for a specific Internet Explorer (Active-X)-based application or website, do not use it to store passwords at all. Do NOT use Internet Explorer for home use or any other reason.

- Cory Lykins
VP of Tech Services
First Network Group, Inc.