Crossing the Digital Divide – Volume 2
by: Joseph Feigon
"Keep it safe"

Do you have Internet access yet? Lest I confuse anyone, the Internet, World Wide Web, Web, Net, are one and the same. I'll keep it to 'web', easier to type.

The web was a University developed project for the military, and was born as Arapanet. The science that made Arapanet (later the Internet) possible is a common language (protocol) for communication between computers - exchanging data, across the fastest possible routes. Those routes consist of copper wires, fiber optic cables, or microwave beams (or any combination therein), in a dynamic matrix throughout the country and planet. It's really quite amazing the wealth of content on the web, accessed with a few clicks of a mouse.

The foundational principle of the web is an open exchange of information, e.g., data packets, or, more simply, requests and responses. The web is a very big place, where truisms remain, the playground vast, the safeguards few. Once you're on the web, the possibilities are endless, as are the risks. Being safe, being secure, and being prepared isn't that difficult.

Most folk have a difficult time with this: the **moment** you connect a tablet, laptop, desktop, xBox, smartphone, even a security system to the web, you are potentially vulnerable. You may not be exposed, but you are visible. Unbeknownst to you, there will be immediate attempts to probe your computer, assess your vulnerability, and capture device information. No kidding. Almost all of these attempts are automated, some to gain access to your device, steal information for resale, or get you to voluntarily give them money through hijack/threat. Some attacks are engineered to use your computer and Internet connection as a relay point to mask their identity. It's real, it's scary, but with a few simple steps, and common sense, you'll be safe.

Here are some simple guidelines that will help protect you:

1) Keep your device software up-to-date.
All devices that can be connected to the web have application and communication software. Software isn't always perfect, imperfections are found, fixes are created. Updates often include performance improvements as well as security fixes. Keep your device current.

2) Create easy-to-use **secure** passwords.
I could fill an entire column with password security tips. We're discussing passwords to banks, health care providers, tax records, shopping sites, county sites, music sites, file sharing sites, you name it.

A good password is easily remembered by you and impossible to crack with software

Most web sites want 8 characters or more, at least one capitalized letter and one symbol. 'io8eiP$0' or 'kooG4#hi' are excellent examples of secure passwords, but are they easily remembered? I think not.

Keyboard symbols include !@#$%^&*()z_-+='";, and the SPACE bar. While not all servers

accept the space bar as a symbol, most do, and using a space will make your life much easier. This is really good news for keeping yourself secure while retaining easy-to-remember passwords.

Here are a few examples of great passwords (easy to remember and hard to break):

"I love Cahto Peak" "101 and One" "My dog is Fido" "Daddy's Birthday" "3 Great Girls" "Greasy Spoons" "25 Main Street!" "$3 Spotted bird". Yup, you got it. Simple two+ word/symbol phrases.

Final note on passwords: Don't make them all the same. Email and Finance never the same. Facebook and Email never the same. It's okay to write down your passwords and pass phrases, be sure to keep the document in a safe place.

Next up: We'll talk about computer hardware, data storage, and recovery from equipment failure.