Crossing the Digital Divide (v38)

"Readiness"

By Joseph Feigon for the Observer

The Internet works around-the-clock, every day, all day long. Acts of Terror and Vandalism can cripple segments of the Internet, hackers and rip-off artists don't care what time of day you sleep, and powering everything off merely interrupts any and all attacks on "you" or your devices.

Shark infested waters, maybe, but it is safe to swim with a few precautionary routines – routines, 'as-in', things to do with some degree of frequency. Better pre-emptive than reactive, right?

1) Keep your PC, Droid, iPhone, xBox, Rooku, and other Internet connected devices updated.

2) Keep your anti-virus and anti-malware software current.

3) Update all your passwords, and don't use the same password across all sites. Make your passwords difficult to decrypt, e.g. "My Password 123" is unbreakable in your lifetime, "MyPassword123" would present little challenge for most hackers.

4) Write your passwords down and keep them in a physically safe place.

5) Enable two-factor authentication wherever possible. Create a secondary email account as a backdoor for yourself, should you lose access to your primary email account.

6) Backup your documents and photos.

7) Photocopy your passport and drivers license (this need only be done once).

8) Create list of your credit cards, account numbers, and vendor phone number.

I've seen a number of "malware" attacks the past few weeks which look like a ransom-attack, always presented as a web page. I've seen the web page, warnings that your machine is infected, call some 855 or 800 number and cough up money to regain control of your PC. Don't. Do. It. Under. Any.Circumstances. It's a non-invasive webpage designed to get YOU to open your wallet. Use ALT+F4 to close Chrome (or Internet Explorer, or Firefox), the "ransomware" shouldn't reappear.

Just to repeat this week's message:

1) Backup stuff you can't replace

2) Update your Smartphone, PC and Internet connected devices

3) Change your passwords and make them strong, setup two-factor authentication

4) Copy important credit card, passport and drivers' license information, store safely

Keep control of those things you can control.