THE HACKERS ARE COMING...

How-To Safely Surf The Internet

Ronald Nutter

Special Edition

This is a special edition of "The Hackers Are Coming… How-To Safely Surf The Internet" for the readers of CSOOnline.com. This is just Chapter One of the full book. The full book is available in either paperback and kindle formats at http://www.ronnutter.com/kpyop.

If you would like a presentation using the content in the book, please contact Ron at http://www.ronaldnutter.com. Depending on the online or cloud based services that your company uses, it is possible that a custom presentation can be created to ensure the audience receives the maximum benefit. For more information, please visit http://www.protectyourlogin.com.

This book is a result of research that I have done and/or products that I am personally using. Product names and/or Company names associated with those products are as I found them. Any resemblance to actual persons, living or dead, or to actual events or locales is entirely coincidental.

Cover Credit: wk1003mike/Shutterstock

TechBytes Press
http://www.techbytespress.com

Version 2016.06.18

Disclaimer
Unfortunately in this world of lawsuits, I want to

make the following disclaimer. Everything that I have written about here is about my own experiences or as a result of research that I did. Your results may vary from mine. What you will read about here are steps I have taken for my own emergency preparations. If I haven't ordered something but found that it was something that I would be looking at in the future, I will indicate that.

Kindle ISBN - 13:978-0-9971133-0-3
Paperback ISBN - 13:978-0-9971133-2-7

Disclosure of Material Connection: Some or all of the links in this book are "affiliate links." This means if you click on the link and purchase the item, I will receive an affiliate commission. This will not affect the price you pay for the item you purchased. Regardless, I only recommend products or services I use or have used personally and believe will add value to my readers. I am disclosing this in accordance with the Federal Trade Commission's 16 CFR, Part 255: "Guides Concerning the Use of Endorsements and Testimonials in Advertising."

Table of Contents

About The Author

Ron Nutter has written for technical trade press since 1990. Over the years he has written for InfoWorld, LAN Times, TechRepublic, NetWare Solutions, Network Solutions and Network World. He has written and produced HelpDesk ToolChest with Ron Nutter for Network World.

The list of people interviewed includes Steve Gibson of GRC Research, Laura Chappell of Chappell University, Chief Twit Leo LaPorte and Dave Ramsey of Financial Peace University to

name just a few.

Over the years, Ron has obtained a host of certifications -

Cisco - CCDA, CCDP, CCNA, CCNA Security, CCNA Wireless, CCNP Security, CCNP Route/Switch
Microsoft - MCP, MCSE
Novell - CNA, CNE, Groupwise CNE, ECNE, MCNE
VMware - VCP5

If you would like to see about reviewing your product for the website, video podcast, audio podcast, or possible inclusion in a book, please contact me at helpdesk@networkref.com. When shipping items for review, please use only Fedex or UPS and send the tracking number so that arrangements can be made for someone to be at the office when delivery is attempted.

Ron is also available for a limited number of speaking and consulting engagements.

Register your book and get notified of updates - http://www.protectyourlogin.com/thac.

Bookmark this link to keep up with new books as they are released - http://www.ronnutter.com/booklist/.

How to use this book

There is a method to the madness in this book. Please take a few minutes to read this and everything else will make sense. The first thing that you will go over are all the tools that are at your disposal to begin the journey to putting the most protection in place that you want for all of your social media accounts.

For those that remember the catalogs of years gone by that had items organized in categories of good, better and best. That is how the steps I outline for each of the sites I mention here are organized. The first level, putting a strong password place puts you at the good level for protecting your accounts. I wrote each of the procedures in the same form under the presumption that you may have some but not all of the accounts that I written up. I assume in each of the steps that you have already selected a password manager app to accompany you on this journey.

Using a single strong password is better than using something like Password or Cisco123 for your account password. Having a unique, strong password is even better. Having a distinctly different password for each account increases the level of difficulty for the attacker by adding another barrier to entry in compromising more than one account at the same time. Taking your preparations to that level gets you to the Better level of your journey. Creating a strong password is something that may not come easily to some. This is where

the right password manager application or even some independent tools built just to help you create a strong password according to criteria you specify in terms of length, use of numbers, and special characters (i.e. punctuation) will help you put together a difficult password to guess for an attacker.

Using Two Factor Authentication, using either a token that has a constantly changing set of numbers on a software or hardware token or a SMS text message with an access code to use, will help you establish a barrier to your accounts that should help put as much protection in place for your accounts as is possible. Don't let this type of protection scare you because of the length of the name. Once you have enabled this on one or two of your accounts and get used to the slightly different login process, you will be ready to pursue that same level of protection for your accounts.

More websites are starting to implement a process where you have to select and provide answers for a series of questions. These questions may be used as an additional step to go through for logging into an account or as a protection step before allowing an account password to be changed. This is another mechanism to have in place for those websites that use it. I will talk more about this in a later section of the book.

Each service type listed in the book is written so that it assumes you don't have any other accounts to register. It is meant to be a checklist to make sure you go through each of the steps needed to

better protect your account.

Before you get started reading this book, keep this next fact in the back of your mind. According to the folks at IDKey (a company you will see mentioned later in this book), it only takes a hacker 10 minutes to guess a 6 character lower case password. That alone should be a good reason to increase the difficulty or strength of the passwords that you currently use.

When you see the word **VIDEO** in a chapter, the URL and QR code that follows directly link to a video on YouTube. This goes into more detail about the chapter you are reading or about the product or technology just discussed. If you want to skip ahead, all of the Videos for this book are in the same playlist on my channel, TechBytesRN, on YouTube. Your first video for this book is below. The other videos will be in the book similar to what you now see.

Watch Video -
http://protectyourlogin.com/trailer

What is the FIDO Alliance ?

I normally don't get that excited about a standards group. The FIDO (short for Fast Identity Online) Alliance is a little different. The group formally launched in February 2013 by six companies to lead the industry by moving from password dependencies to strong authentication which is more secure, private and easier to use than passwords. Of the companies that I provide how to use Two Factor Authentication with in this book, it should be noted that Paypal was one of the founding members of the alliance and continues to remain involved.

Who would think that a year later, you would see the membership swell by to more than 100 companies including Google, Microsoft, and Netflix to mention just a few of the members. The number continue to grow, sometimes daily. When I checked the current membership list in October 2015, it was well over 225 members and shows no signs of stopping. Take a look for yourself to see the level of involvement and who is involved - https://fidoalliance.org/membership/members/. When this many companies are involved, we all win with this level of cooperation.

One of the first ways that I heard about FIDO was when I initially heard about one of the members of the FIDO Alliance, Yubico. I had a long conversation with the CEO and Founder of Yubico, Stina Ehrensvärd. Our conversation lasted for almost 45 minutes and was the best education I

have ever received on a technology that was new to me.

The adoption of FIDO is continually growing. The FIDO 1.0 Standard was released on December 9, 2014. Since that time, Microsoft has announced support in Windows 10. NTT DOCOMO, deployed FIDO authentication for its subscribers in Japan, becoming the first Mobile Network Operator to deploy that technology. Dropbox, a well know cloud storage company, recently announced it's support for FIDO and has made it available to its users. Github has announced that it will accept FIDO U2F authentication on its popular code-collaboration service.

Most of the ways I show you in this book on how to protect your online presence are provided by FIDO members (Yubico, for example). As I find other FIDO certified products that are a good fit, I will update this book as those solutions become available. Here is a YouTube video that I would encourage you to take a look at to get a good understanding of what FIDO is and how it can help protect you. Here is a page that will have the latest videos that show other uses of FIDO certified products - https://fidoalliance.org/adoption/videos.

CHAPTER ONE

Tools

What tools are the best to use ?

What I will outline in this part of the book will be the tools I have looked at and from those selected the ones that worked best for my situation. There is no one solution that will work for everyone, so I wanted to provide you a list of what I had looked at to save you some time when you are looking for the combination of tools that will work for you.

Your first stop is to select a Password Manager. I had tried several open source ones when I first started using one several years ago. The ones that I had looked at were a little clumsy in the area of file synchronization area. When I was able to work around that, dealing with delta changes was a little more challenging. Delta changes are when you make change A on one device and change B on a different device and getting them to apply in the correct order when synchronizing all devices so that the changes where applied in the right order.

You will read about Two Factor Authentication. Don't let the term scare you. It is the next step beyond username and passwords to access a site/service. Using a strong password will only protect you so long. It is just a matter of time and resources before someone with the right tools and determination before a password can be cracked. Using Two Factor Authentication increases the level of difficulty to the point to where only the most determined hacker may try to stick it out. Since they have bills to pay as well, they will only spend so much time without having any financial gain.

When using Two Factor Authentication, you will need to look at using either a Software or Hardware Token. I have used both and they each have their own pluses and minuses. Having dealt with the costs of a hardware token from one of the well known commercial Two Factor Solution providers, I initially shied away from that option. That was until I had the chance to talk to Stina Ehrensvärd, CEO and Founder of Yubico. Using the Google Authenticator client was as safe as I thought but once someone had my device that the Authenticator was installed on, they essentially had the keys to the kingdom for accessing all of my Two Factor enabled accounts. That is what got me to start looking the Yubikey solution. Once I got a Android smartphone containing NFC, I was able to experience the full Yubikey solution. I get the advantage of a Two Factor software token with the security of a Hardware Token.

If a site doesn't support fully support Two Factor Authentication but offers you a SMS or Email with an access code, that is better than nothing. The challenge with using SMS is that depending on what provider is being used to send the SMS message to you could result in a delay of several minutes before you get the code needed to complete the authentication process.

Crafting a strong password is not something that comes easy to everyone. That is complicated by some websites not allowing you to use special characters that some of us would know as punctuation. There are a variety of tools available,

some available in the password managers that I talk about in this book, to help make that process a little easier. One rule that I am doing my best to not use the same password on multiple sites.

One recent account hack that I learned about was using answers to security questions that some sites use as an additional level of protection to make sure that only the actual account holder is requesting a password change or as another step in the login process. The problem is that in the case I am familiar with, the answers to the security questions could be readily found in information available online about the account holder. Depending on how public of a persona that you already have, or may have at some point in the future, giving the correct answer could make it one step easier for someone to gain access to your accounts. The two ways that you can answer the security questions and help avoid this will be to give either inaccurate answers or give an answer that is a series of letter, numbers and functional or special characters. In either case, be sure to record both the question and the answers you give for that sites entry in the password manager that you decide to use.

Password Managers

mSecure

http://protectyourlogin.com/msec

This is the password manager that I have used for several years. I had used a variety of open source password management apps but the problem I ran into was that they were only for the PC or had a file that had to be manually copied between machines to keep the passwords in sync between systems. That is what attracted me to the mSecure software family. It supports just about every platform that you would probably run into on a daily basis.

You have two different options for keeping your logins and passwords in sync. The first involves having all the devices on the same wifi network. That is sometimes easier said than done. What I have implemented is syncing the password file to my Dropbox account. In that way, whenever I bring up mSecure on whatever platform I choose, that I automatically have the latest password file

available for use. The real silver lining in this is that if I have made multiple changes on the same or different logins, mSecure applies the changes in the chronological order they were made in.

LastPass ****

http://protectyourlogin.com/LP

LastPass is a cross platform password manager. To really get full functionality, you will need to subscribe at the Premium level (as of September 2015, that is $12 per year). For that amount, you get the ability to have unlimited sync across an unlimited number of devices. You also get the ability to support more MultiFactor Authentication systems such as Yubico and biometric options. Priority support come with this package. If you operate this on a locked down computer, you will also have the option LastPass from a USB drive when at the Premium level.

keeper®

http://protectyourlogin.com/Keeper

Keeper Security is a multi platform password management and security tool. Pricing has two different levels - $9.95 give you password sync with one device. You also have the ability to add additional cloud file storage. For $29.99 a year, you get the ability to sync multiple devices.

http://protectyourlogin.com/DL

There are two price levels - free and $39.95. The main distinction in one device on the free plan and multiple devices for $39.95. All platforms except for Linux are supported.

http://protectyourlogin.com/1pass

All platforms except for Linux are supported. The Windows and Mac clients are fully functional for 30 days. The licenses for Mac and Windows start at $49.99. There is a charge for upgrade that varies depending on the situation.

SplashID Safe

http://protectyourlogin.com/splash

There are two versions - free and two different levels of pay (monthly or yearly). Pro users get automated backups. The last 5 backups can be downloaded and restored. All platforms are support except for Linux. By implementing the Chrome extension, you can integrate SplashID Safe

functionality directly into the browser.

Software Tokens

Google Authenticator

Watch Video -
http://protectyourlogin.com/ga

This is the first two factor client that I got started with. It is easy to use and is something that you will have something up and running in a few minutes. This is intended for a phone that has a camera in it cause you need to capture the QR code that is displayed as a part of the two factor enrollment process.

One suggestion that I found out about that has proven very helpful is to do a screen capture of the QR code used for each login that you will use this, or any of the two factor clients that I will talk about in this eBook. Put that screenshot in an Evernote folder or whatever app you use to keep track of

important items. Label that screen shot as to what website it is for and the date you started using it. This is available on both Apple and Android platforms.

This is the latest two factor client that I have found. Of all of them, it is the closest to being a swiss army knife in that it does a little bit of everything. What separates this one from the others is what it can do beyond just giving you a 6 digit code for login verification. You can add an additional software component that you can either scan a code with the SAASPASS app or click the Remote Unlock button for that computer in the Computer Login Section of the app.

When you add a website login, when possible, SAASPASS will also put an appropriate graphic for the site to help you quickly identify it from the list of the other logins that are already in the list. This is available on both the Apple store and Google Play store.

Authy

This was the first two factor client that I found after I had been using Google's Authenticator client for a while. What distinguishes Authy from Google's client is that it backs up the tokens you have it configured for to its own cloud. In addition to that, it also makes sure that the device that is running the Authy client is on the correct time so that you don't have unpredictable results caused by a different in time references. If you are converting from Google Authenticator, there are instructions on Authy's website to help you make that transition. This is available from the Apple store and the Google Play store.

Symantec VIP

This two factor client isn't as widely used as the other two factor clients I have listed above. I have seen this used mainly for eBay and PayPal. If you go with this 2FA client, there will be a token serial number that you will want to record. You will want to make sure you have your contact and recovery information up to date. During an upgrade to my smartphone, the token serial number changed and I didn't catch it. My first indication of a problem

was when I lost access to getting into either of the accounts I had it configured for. It took about 20 minutes on the phone with an understanding customer service again to gain access to my accounts and setup a new security token. This is available for both Apple and Android users.

Yubico Authenticator

Watch Video -
http://protectyourlogin.com/ya

This client is just one part of a three part solution. In order to get this to work, you will also need Yubico's NEO token. You will need a phone that fully supports NFC (Near Field Communication). At the point, this means that only Android phones can be used. While Apple does have NFC support in the iPhone 6 and later, it can only be used with the Apple Pay system. I have

successfully used the Yubico Authenticator on my Google Nexus 6 phone This app can be downloaded from the Google Play store.

Hardware Tokens

Yubico U2F

This is my go to hardware token. I became aware of this token when I was writing a previous book. I had been using the soft token client released by Google. After a long talk with the CEO of Yubico, Stina Ehrensvärd, I learned of potential security issues with software only clients. The biggest one was that when using a soft token and the phone that it was used was stolen, you have just given a major component to your account security to someone who will use it for no good. This is when I started using the Yubico key.

I always like to have a backup plan in everything I do. Imagine my surprise when I learned when setting up the U2F Special Security Key that, at least on Google accounts, that I was able to assign multiple keys to the same account. This is handy as I can have one key at home and another key with me and be able to get into the account without having to get the wallet the one key is in. Use the QR code below or click on the

URL to purchase your own key.

There is one item you need to know about. The U2F functionality only works with Google's Chrome Browser at this point. I have been on a conference call where Yubico talked about working with Firefox, IE and Edge. That is work in progress and dependent on third parties so there isn't a definite day when this functionality will be available on other browsers but there is at least a roadmap for this happening.

http://www.ronnutter.com/yubu

Yubico VIP

When you are purchasing an item in an auction you just won on eBay or paying someone using your PayPal account, this is the key that you will want to use. There is a soft token that you saw mentioned in the previous chapter but that can have it's own challenge as you can see. This token is supported by both eBay and PayPal. Due to a security requirement of the Symantec authentication system that both of these sites use, the functionality needed for the key to work can only be implemented at the time of manufacture. Be careful about making any changes to this key as once you have deleted or damaged the functionality needed by eBay/PayPal, you will need to purchase a new key. Even though Yubico has other blank hardware tokens, you will notice a large checkmark on the back of the token. Use the QR Code below or click on the URL to purchase your own key.

http://protectyourlogin.com/yusy

Yubico NEO

This is the latest key in the Yubico family that I have been working with. The graphic you see is actually two different keys. The NEO is the larger of the two keys show. The NEO-N is the smaller key. I have been using the NEO with my Google Nexus 6 with some very interesting results. Since the NEO supports NFC as well as my Google Nexus 6, I can use this key in conjunction with the Yubico Authenticator (available from the Google Play Store) to access all of my accounts that are protected with Two Factor Authentication (with the exception of eBay and PayPal because they use a different system). I bring up the Yubico Authenticator app on my Nexus 6 and tap the Yubico NEO on the back of the phone. It immediately populates the screen with all of the tokens I have programmed it for. Once the currently displayed values expire, I have to tap the NEO on the back of the phone to get updated values displayed. If I share the phone with someone, I can either let the current keys expire (they will turn grey on the screen) or reboot the

phone to clear the codes from the screen. Use the QR Code below or click on the URL to purchase your own key.

Yubico has heard requests for supporting Apple users. The problem appears to be with Apples implementation of NFC. They are working on a different key with Bluetooth support that will work with the iPhone. I have requested to be admitted to the beta test program. At this point, I am waiting to receive a device to test with. I will update this book when that has happened.

http://www.ronnutter.com/yune

Yubikey 4

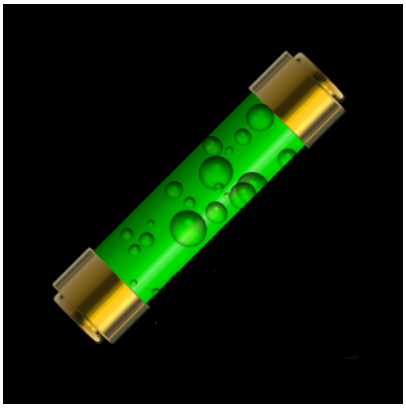
This is the latest addition to the line of Two

Factor Keys from the folks at Yubico. One of the big differences with this key is that you have the option using most of the major browsers instead of only being able to use Chrome. This key has the potential of setting a new standard in functionality since it supports supports multiple authentication protocols, including Yubico OTP, smart card (PIV), and FIDO U2F.

The Yubikey 4 key is supported by the following password manager applications - Keepass, Password Safe, LastPass, Password Tote, pwSafe, and PassPack. Another advantage to this new key is that you have the ability of using it as a source of two factor authentication for Full Disk Encryption. The folks at Yubico have a pdf available for download on their site going through the process of integrating the Yubikey with Full Disc Encryption to get you started on that path when you are ready.

http://protectyourlogin.com/y4

Injector



This particular solution is one that is hard to classify. Here is why - it is part hardware and part software. For the app that resides on the phone, it is a password manager but when you pair it up with the matching Bluetooth LE adapter, you have a solution that can automatically send just your password or username and password, depending on how you have it configured to work. When I first found this solution, I tried with two different bluetooth sources seeing if it would work with any bluetooth device and found that it wouldn't. This is good and bad. It would be nice if you could use the existing Bluetooth adapter present in most laptops. On the other hand, by using their adapter, a higher level of encryption can be used between the smartphone/tablet running Injector app and the Injector BLE adapter.

What got my attention was that this was the first solution I had found that had multiple browser support. At this point, it support Safari and Chrome. Firefox is on the roadmap but there was no date I could find on the website to indicate

when it would be available. Most of the solutions I have found up to this point currently only support the Chrome browser.

Once I got one of the two Bluetooth LE adapters from the folks at Password Injector, I got the chance to really see the potential of this system. It took a little getting used to from a configuration standpoint but I think you will be pleased with what you see. During the credential setup process for a particular service/site, you will need to scan the QR code for the information needed to generate a OTP (One Time Password) used for sites that allow you to use Google's Authenticator or similar apps. This is where having a screenshot of the QR code when you initially setup the login for two factor authentication will be handy. A nice side benefit of using the Injector app for 2FA (Two Factor Authentication) is that unlike the other apps that I have looked at for this purpose, it doesn't display the code on the screen. The only time you will see the code is when the code is sent to your computer when the Bluetooth adapter is installed.

http://protectyourlogin.com/painj

Watch Video - With 2 Factor
http://protectyourlogin.com/piupt

Watch Video - Username & Password
http://protectyourlogin.com/piup

IDKEY

The IDKey is the first hardware token that I have found that supports use of biometrics (i.e. your fingerprint) as a method of authentication when

logging in to a supported service. It supports both Bluetooth and NFC which means that it should be an option for both Android and iOS users. I will be writing more about this device when I receive one and can show you how I have implemented it.

http://protectyourlogin.com/idkey

Email and SMS as Two Factor Tokens

With some websites, getting an email or SMS message with the OTP (One Time Password) to use for this particular login attempt is your only option. While not idea, this is better than nothing. Which will work best for you depends on how much you travel. If you travel out of the country, getting a SMS message may be problematic (and possibly expensive) since getting a SMS message can difficult when you are operating on a different carrier in another county.

If you only have a SMS message as a method for delivering the authentication token, consider getting a Google Voice account. This gives you an option for getting the SMS message via an email. While not ideal, it is an option worth thinking about.

Crafting a strong password

Creating a strong password isn't one of my favorite things to do. There are several ways that you can make the process a little less painful. Someone I worked with several years ago taught me a trick that has served well on several occasions.

Take a password that more than one of us has used, our old friend "password". With a few changes of upper/lower case and punctuation and you can have something that looks like P@s$w0rD. You can make it a little more challenging by adding an exclamation point at the end and even a few number, in no particular order of course. What you want to avoid is having a password that could be guessed using what is known as a "dictionary attack" where a series of passwords is tried using the words right out of a dictionary.

If you want to make it a little more challenge for an unwelcome intruder, most password managers offer the ability to come up with a randomly generated password as a part of the process of entering the information about a particular login that you want to keep track of. I have run across some websites that won't let you use "special characters". That usually seems to mean punctuation letters. The website should just say that instead of making you guess what they don't want to use. In addition to the password manager, there are also several apps available for both Apple and Android phones that can help you come up with a challenging password as well.

Watch Video -
http://protectyourlogin.com/gsp

Account Security Questions

More websites are starting to ask one or more questions that you can answer that can be used as a secondary challenge during the login process. In some cases, these same questions can be used as a part of the process you can go through when you have forgotten the password you setup for the account. Some sites may allow you to choose from a list of questions to have in your profile or even allow you to enter your own questions.

There is something that you need to think about when both selecting an answering the questions. While our basic intent is to answer a question with a response that we can remember, you may want to think a little differently about that. One reason to do so is that some answers you might provide, in this day of being able to find just about anything about yourself on the internet, you need to think about providing an alternate answer that doesn't match what can be found about you. For example, if one of the security question options ask about your place of birth and you were born in New York, pick another city/town such as Orlando or Knoxville in an area of the country where you haven't lived or isn't geographically near where you currently reside or where you were born.

If you feel up for the challenge, you can think about taking it to the next level. Some websites offer a wider variety of questions to choose from. One thing to think about is to not use the question for where you were born on every site where that is

an option. Depending on the number of sites up have accounts on, you may not have a large variety of questions to choose from. The point here is to make it challenging enough to encourage someone attempting to access your account to go elsewhere.

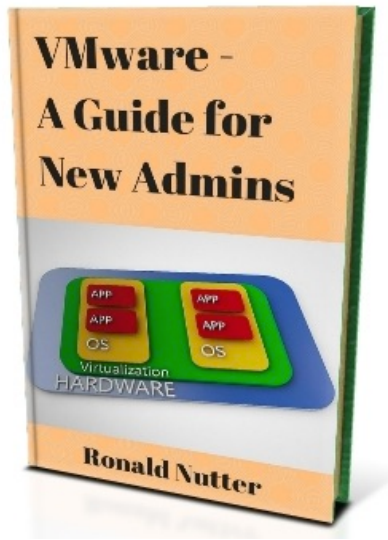
Keeping track of both the questions chosen and the answer you gave for each question, should be kept in a note field in the password manager app you use. Depending on application you have chose, you might want to think about setting the note field as a "sensitive" field. In doing so, it helps keep someone from looking over your shoulder and learning some of your answers. Depending on how sophisticated your application is, you could have the question be in plain text in one field and the answer be hidden in a sensitive field right below it. In that way, you would have one more layer of protection about the answers you have used.

What may be easier than using alternate location names is to use a random set of letters and numbers instead of a plain text answer such as the name of a city or brand of vehicle you had. This increases the level of difficulty of someone successfully guessing your answers or finding the answer on a social media site or by the use of a search engine. The importance of either using a false location or random letters for an answer recently hit home with a well known internet marketer. Every time the security questions were used to regain access to an account, the attackers knew about it because they were watching the

email account for this internet marketer. After the password and been changed, they had changed it back to something they knew moments later. It took approximately two weeks to figure out how the hackers kept getting access to the accounts to put a system in place like I have outlined here to put a stop to their activities.

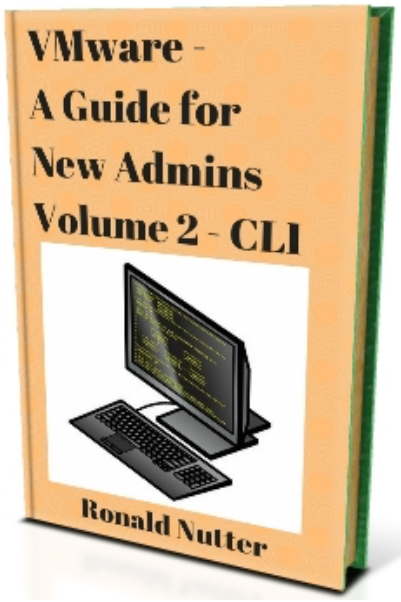
In addition to using false or misleading answers for security questions, also implementing a two factor solution from vendors such as Yubico or Password Injector from Bluink Ltd, might have prevent the situation from happening to begin with. While using a strong unique password for each website or service is important, that is just one tool in protecting your accounts from being taken over by someone else. The more steps you take now, increases the level of difficulty for someone trying to break into your accounts.

Please check out my other eBooks and add them to your library today !



This book is targeted at the new VMware Admin or someone who has been out of the field for a while and needs to come up to speed fast. Think of this as an electronic notebook with things you won't learn in a VMware class. If you are looking for a job in this area, some of what you find here might just make you stand out from the others interviewing for the position.

http://www.ronnutter.com/vmna1



If you have dealt with any type of technology, you will know there are times when using the GUI won't work. This book gets you familiar with the different ways of accessing either a VMware host, vCenter server or VDP appliance. Knowing how to navigate around the Command Line Interface in the VMware product family is a handy skill to have.

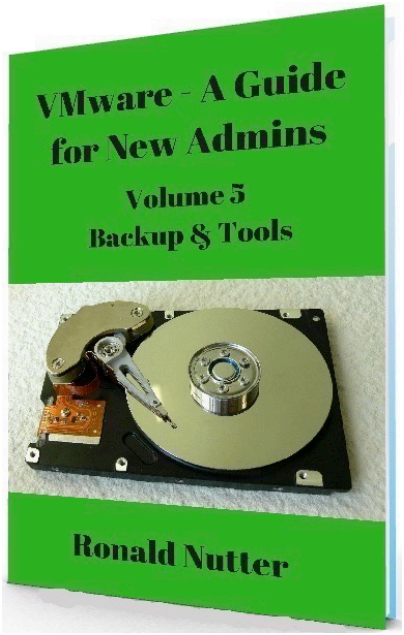
http://www.ronnutter.com/vmna2

At some point in your VMware career, you will need to do at least on upgrade. While no two upgrades may ever be the same, having a rough blueprint will make the process a little easier. This is another area where doing a dry run in your lab will help give you an idea of what to expect in the real world. Running into problems in the lab is easier to deal with than in a production environment.

http://www.ronnutter.com/vmna3

In volume 4 in the VMware - A Guide for New Admins series, I put together a timeline for those with little to no background in VMware to help them get started on the path on learning VMware and a new job skill. This book will be updated as I release additional books in the series to continue the buildout of the path for increasing your VMware skills.

http://www.ronnutter.com/vmna4

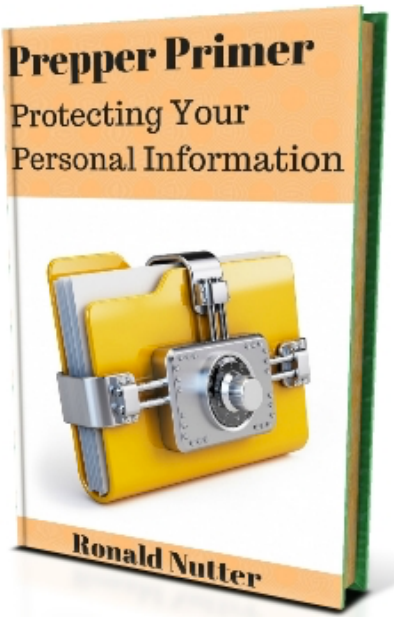


This book is targeted at the new VMware Admin or someone who has been out of the field for a while and needs to come up to speed fast. Volume 5 deals specifically the different things you need to think about in backup up your growing VM farm. This is another area where you will need to be well versed in.

http://www.ronnutter.com/vmna5

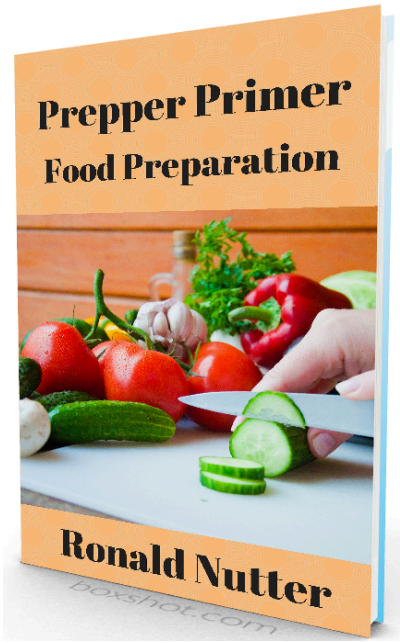
You can't always depend on a cell phone during an emergency or disaster. This book covers a variety of options such as Satellite, Amateur Radio, MURs, GMRS and several other options. One thing you need to read about is how to use your cell phone to establish your own private texting network !

http://www.ronnutter.com/ppv1c



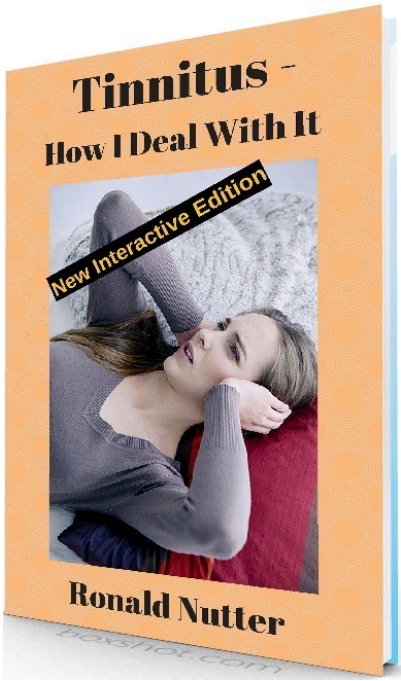
This book covers steps you will need to take to protect your personal information during a disaster. This is a prime time for identity thieves to strike. This will also be the same time when you will have the least time and resources to deal with the situation.

http://www.ronnutter.com/ppv2p



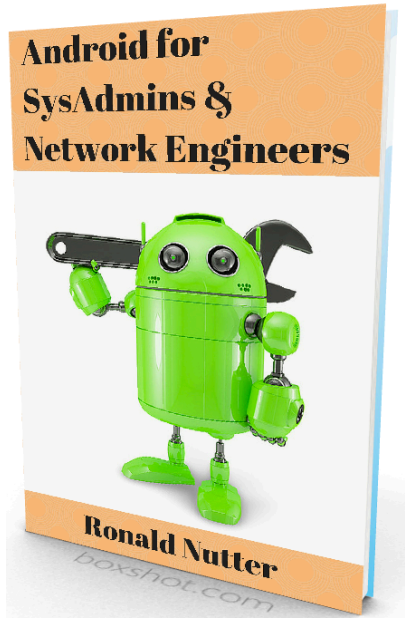
Depending on the length of a disaster or emergency situation might mean that the grocery store(s) near you will be low or out of food. Know how to do some basic food preparation steps or even growing some of your own foot before a problem occurs will help you be that much more self sufficient for the duration of the disaster/ emergency and as a matter of general principle.

http://www.ronnutter.com/ppv3f



It is estimated that somewhere between 1 and 5 to upwards of 50 million people suffer with Tinnitus, otherwise known as ringing in the ears. In the past, there wasn't much that could be done to treat Tinnitus as there currently is no cure for the problem. That all changed in early 2014. This book is a diary of my journey since being diagnosed with Tinnitus and what I have learned along the way.

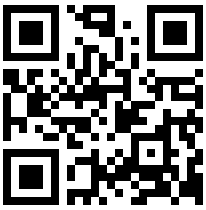
http://www.ronnutter.com/tims



Android isn't just an operating system for your phone or tablet. There are a variety of apps that can turn your device into a ad-hoc network testing tool so you don't have to carry a war chest of testing equipment and tools with you. With the tools listed here, you can be ready to troubleshoot at a moments notice !

http://www.ronnutter.com/asne

As the stories continue to show up in the press about websites being broken into or accounts being hacked, you can have a variety of options to look at to protect yourself. There are a variety of options that until recently were available only to medium to large commercial clients. This book walks you through step by step on ways that you can make your accounts just hard enough to try to break into that the hackers will look elsewhere for easier less protected targets.



http://www.ronnutter.com/thac

Ronald has written for technical trade press for over 20 years.

Please Check out http://www.ronaldnutter.com for the other books he has written.

There are several things that you can do to prevent your account being taken over by others. Depending on the social media account or online service that you want to protect, you can increase the level of protection between the hackers and you in as little as three steps.

Look at it this way, would you rather spend a little more time and some money protecting your accounts today or countless hours and a lot of money fixing the problem after the damage has occured ?

Keep up with the latest information by going to http://www.protectyourlogin.com today !

TechBytes Press
http://www.techbytespress.com