Technology Safety

Contents

• Slides 4-5	Discussion
• Slides 6-7	Basic Thoughts
• Slide 8	Learning
• Slide 9	Levels of Security
• Slide 10-11	What to look for
• Slide 12	Smart Devices

Contents

- Slide 13 Phones
- Slide 14 Two Factor Authentication
- Slide 15-16 VPN
- Slide 17 Password Manager
- Slide 18 Social Media
- Slide 19 Am I Infected
- Slide 20 Secure Communications
- Slide 21 Terms
- Slide 22 Final Thoughts
- Slide 23 Happy Ending

Discussion

- Some of the items in this Pub may be a bit difficult to understand etc. I am here to help and will do my best to give you specific info if you ask.
- I will discuss many things in this publication and then provide specific information on selected topics later. I will mark the specific topics in blue.
- It is important for all users to take some responsibility in their use of technology. I suggest each user set up a plan for doing the basic safety actions with their Devices. I usually pick Friday and do my scans of all my devices. I don't rely on automatic or security software that most modern malware turn's off.
- I have created a Database for Vocabulary on Ratsupport.com to try to help users with the problem of terminology and understanding the Tech World.
- I realize that there is no 100% safety factor, Silver Bullet or procedure, you can only do your best, but I will try to give you some things to think about.
- Something I suggest to all, be a Leader and not a Follower, If your kids or friends want you on Facebook, TicTok etc. don't do it, tell them if they want to talk with you, "use MeWe or Truth Social and even X might be getting better and safer".

Discussion

- One thing to think about is, should you have a smart device like a phone or tablet ?
- Should you use a VPN ?
- Should you pay your bills online ?
- Should you have a password manager ?
- Should you use Social Media ?
- Are you part of the solution or part of the problem?
- What you might look for in your emails and SMS text messages.
- Should I use 2 Factor Authentication ?
- Unsolicited contact via Email, Phone, Text etc. What should I do ?
- National No Call List.
- What to do when you suspect you are Infected with Malware.

Basic Thoughts

- Make sure your Modem/Router has a very strong password. I suggest at least 8 characters and include at least one Cap, Lower Case, Number and Special Character. I have an example I don’t think you should use (Pa55w0rd%).
- Look for https:// and a icon of a lock in or near the URL of your Browser. Do not go to websites that do not have this. Https:\\ means you will be using the secure socket layer (safety). Http:\\ is no longer safe.
- Don’t keep your passwords on sticky notes attached to the wall or your monitor. Put them into a notebook and store it out of sight.
- Don’t make a spreadsheet with your passwords and store the file on your computer. If you must use this method then I suggest you put the passwords on a USB Memory Stick and only plug it in when you need the info and then remove it.
- Please realize that Google, Microsoft and Apple are business and they are there to make money and not to help you, no matter what their propaganda is. I try to use applications that are not theirs as this does provide a small safety factor. This said I do use applications from both Google and Microsoft as I find some of real value.
- In general there are alternatives to the default way of using technology, I suggest you take a little time, do homework as I like to refer to it and see if you can save some $$ and be more secure. Please remember the most widely used application is also the one that most apt to be hacked.

Basic Thoughts

- The using of smart devices is not bad or real dangerous as long as you have put some thought into their use. An example is, I use Amazon Echo devices all through my house. I use secure passwords and recently got a VPN that encrypts the data. These devices make life less stressful and they do save some $$.
- We are all subject to slick talkers and people trying to get you to click on something. If it feels bad or makes you uncomfortable, I suggest you back up and give your actions some thought. Please remember there is no such thing as a free lunch, free applications etc. If it is too good to be true it probably is bad.

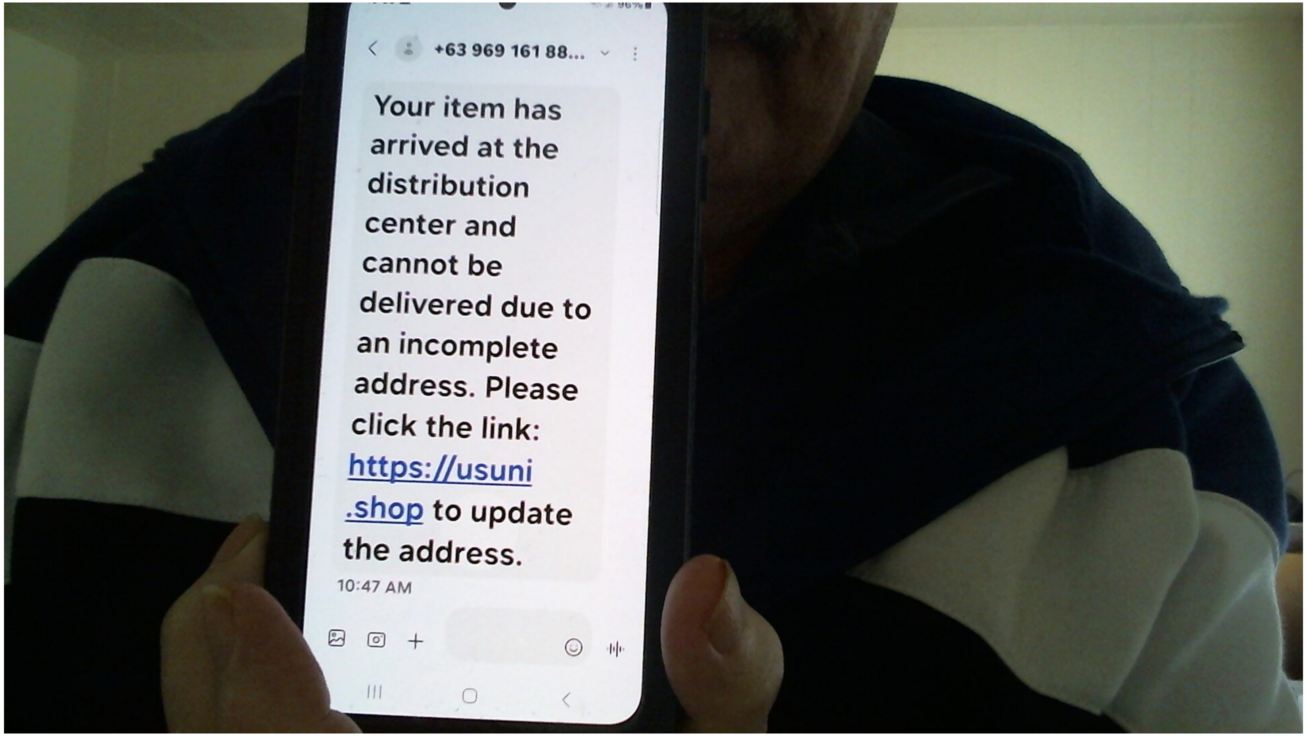
Learning

- I put this section into this Publication in hopes it will help users get a handle on Tech Stuff.
- 1st, almost all people have more than enough smarts to use Technology, for some the problem is technique and not smarts.
- Suggestion: Think priorities, put your learning first and learn the vocabulary and use it in your thoughts and talk.
- When forced we all learn to get by, I suggest take hold of a problem or Tech Device and spend the home work time to LEARN about it and how to use it securely.
- Please don’t try to memorize something, I suggest use and learn and use again until it becomes something that is like driving a car.
- It takes time, I set aside 15 to 30 minutes a day to learn something new. This time is my Learning time and I don’t let other things get into the way. One item or piece of knowledge each day will give you 360 in a year.
- I have a document that tells the story of my getting and trying to use my VPN, it is not pretty, if you are interested contact me and I will send it to you.

Levels of Security

- There is no perfect world and no perfect Security either in life or Technology, we can only do our best.
- Convenience is a factor, so it takes balance in our approach to Tech stuff.
- If $$ is a factor, then we should all take some time out of our busy day and put some effort to our security, Do Scans of Devices, Investigate new approaches and apps to help make us more secure.
- I have Blink Camera’s at my house for security, I use anti-virus, anti-adware software and do the necessary scans on a regular basis. I have recently started using NordVPN on my devices and it seems to make me feel more secure. I would love to discuss the reasons I am using it, but that is for another time or conversation.

What to look for



+63 969 161 88...

Your item has arrived at the distribution center and cannot be delivered due to an incomplete address. Please click the link: https://usuni.shop to update the address.

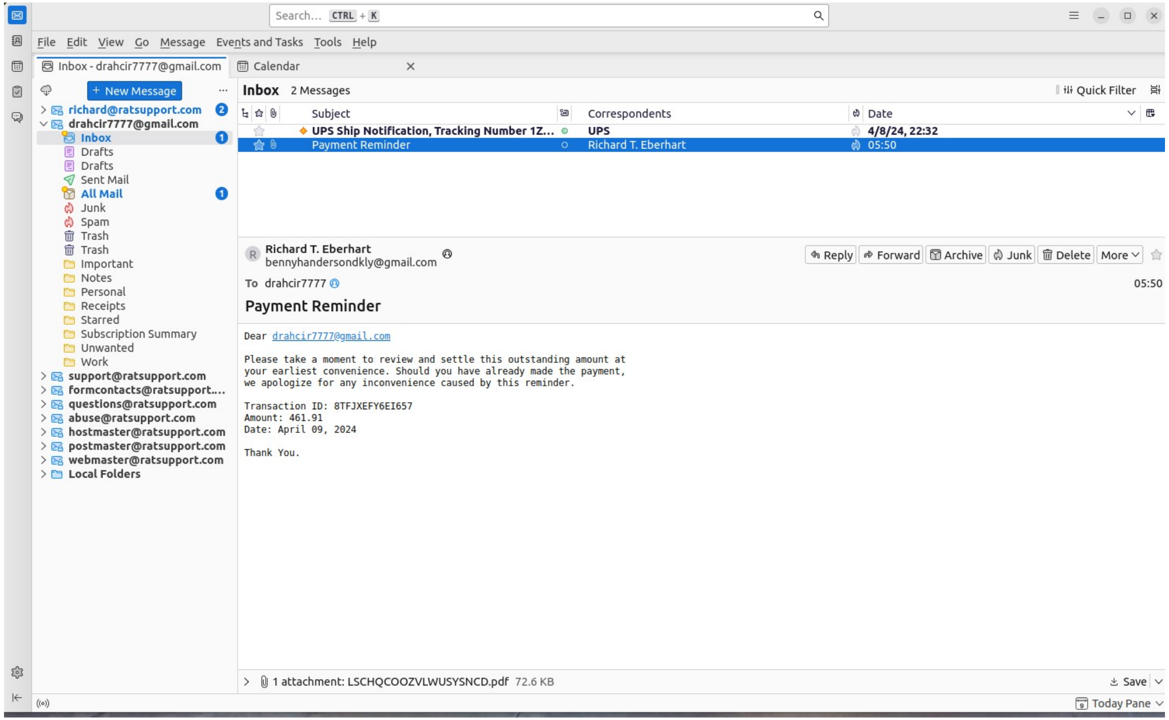
10:47 AM

This is a text I got from someone trying to get me to click on the link.

I don’t know this number, I don’t know this company and I am not expecting anything from this person or company.

I blocked this number on my phone and deleted this text.

What to Look For



Subject	Correspondents	Date
UPS Ship Notification, Tracking Number 1Z…	UPS	4/8/24, 22:32
Payment Reminder	Richard T. Eberhart	05:50

Richard T. Eberhart
bennyhandersondkly@gmail.com

To drahcir7777

05:50

Payment Reminder

Dear drahcir7777@gmail.com

Please take a moment to review and settle this outstanding amount at
your earliest convenience. Should you have already made the payment,
we apologize for any inconvenience caused by this reminder.

Transaction ID: 8TFJXEFY6EI657
Amount: 461.91
Date: April 09, 2024

Thank You.

1 attachment: LSCHQCOOZVLWUSYSNCD.pdf 72.6 KB

I use Thunderbird to manage my email, addresses and calendar.

This suspicious email showed up today and I marked it as Spam (Junk) and deleted it.

I don’t know who these people are and I don’t know the email address and I have not ordered anything from them etc.

If you notice I have a number of email addresses and most are for my work, I suggest all people have at least two email addresses from different suppliers.

Smart Devices

- Most Every person over the age of 18 should have a smart phone or smart tablet as they are actually a bit of a security device when it comes to 2 Factor Authentication.
- If you have an application or account that has access to the internet and you are required to login, I strongly suggest you enable 2 Factor Authentication.
- They can also help with security via camera’s connected to your Alexa app and telling you there is a problem or person at your door etc.
- As with all devices connected to the Internet I suggest you use some type of malware software. There are many but Malwarebytes comes to mind as it connects to most devices.

Phones

- First thing I want to tell you is that the propaganda that Apple Corp. puts on you is just that. One of the latest Malware's was on the Apple App server and being loaded on many Apple Devices.
- It is important that you keep your device safe by using either the Finger Print, Facial Recognition or as I use a good pass code. Don't be caught without one :-).
- Make sure you understand and have activated your find my phone app.
- I suggest you use the Speaker when you can as it keeps the phone a bit of distance from your head.

Two Factor Authentication (2FA)

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves.

2FA is implemented to better protect both a user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically, a password or passcode. Two-factor authentication methods rely on a user providing a password as the first factor and a second, different factor -- usually either a security token or a biometric factor, such as a fingerprint or facial scan.

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

This is where your smart phone or tablet device helps out. In today’s tech world there are hackers out there trying to get your info and it is a good idea you stay ahead of them by using newer tech to stop them.

I have had to implement 2FA on my website and am always looking for new ways to improve safety to the users of my site.

VPN

- A VPN, which stands for virtual private network, establishes a digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet. This ensures that your online experiences are private, protected, and more secure.
- By its very definition, a VPN connection is:
- Virtual because no physical cables are involved in the connection process.
- Private because through this connection, no one else can see your data or browsing activity.
- Networked because multiple devices—your computer and the VPN server—work together to maintain an established link.
- Now that you know the meaning behind VPN, as well as what VPN stands for, let's explore the many benefits of a VPN, and why it might be advantageous to use one.

VPN

- For anyone seeking a safer, freer, and more secure online experience, the benefits of using a VPN are many. A VPN protects its users by encrypting their data and masking their IP address, leaving their browsing history and location untraceable. This greater anonymity allows for greater privacy, as well as greater freedom for those who wish to access blocked or region-bound content.

Password Manager

- A password manager (or a web browser) can store all your passwords securely, so you don't have to worry about remembering them. This allows you to use unique, strong passwords for all your important accounts (rather than using the same password for all of them, which you should never do).
- There are many and by using the mid value NordVPN I go a very good Password Manager. I have also used the password managers in my browsers and 1 Password.

Social Media

- This is a big problem for most. As the bad people and Politicians got involved the whole reason for Social Media got turned on its ear.
- Now some sites like TicTok that is controlled by the Chinese Gov and provides much propaganda and limits free speech exists.
- There are some new and interesting new sites that provide the ability to converse with friends and family with much less interference like MeWe. Facebook, Instagram and others are taking advantage of your existence on the internet and selling your info and making much $$ on you without you even knowing. They also only show their perspective and don’t allow for a broad range of idea’s.

Am I infected ?

- I have a whole Publication on this question in my Members Only Area under Education, Software and Virus. It would be nice if you signed up and took a look at it.
- A quick thought is, If you see something you have not seen before or your browser has changed or your machine has slowed down, there is a good change you have some malware effecting your machine.
- The best thing to do is to run the scans on your already installed anti-virus, anti-adware, anti-malware software. Please do not try to continue with what you were doing and compound the problem.

Secure Communications

- Your SMS messaging and some email are not secure and can be captured. Be aware of what you are doing and how you are doing it.
- Ratsupport.com’s Members Only Area has secure communications and file transfers.
- A number of the Databases used on Ratsupport.com have a secure messaging system.

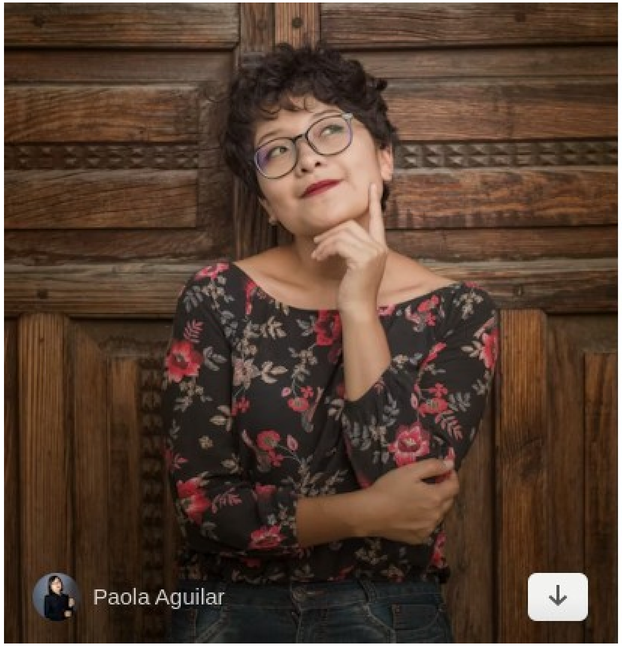
Terms

- I have a Vocabulary Database link on my Ratsupport.com's main page.
- Please take advantage of this tool to help learn the terms associated with today's Tech World.
- If you know a term or have comments about the database please feel free to contact me.

Final Thoughts

- Beware of Propaganda from Companies. It is a same that many like to take advantage of their users for various reasons.
- There are many sayings that should guide us through this Tech World but many of us just don’t take the time to dig down and get to the real truth.
- Please take the time to investigate anything that gives you any pause or questions before you just plunge in and get a result that you did not want or expect.

Happy Ending



I sure do hope this Publication helped you with your Technology Devices and more.

I hope you decide to join the Ratsupport.com's Members Only Area so you can see many more publications similar to this one.

I am very open to comments, helpful hints or advise on this or any of my Publications. I create them to help people with their Technology and to keep me busy :-)