Accounts, Passwords, Security

Or

Ugh!

CONTENTS

1 INTRODUCTION

Remember the days when you could leave your front door unlocked all day and not have to worry about a thing? The worst break-in you might have experienced was a neighbor having returned a borrowed set of pie tins.

Alas, those days are gone. Now, get an account and password for any computer application, you have to go through bunch of screens, answer questions, go to your email or smartphone, confirm that you are who you say you are, and (hopefully) pick an account name that nobody has already picked.

Then comes the evil screen where you have to pick a password. How hard can it be? After all, they give you hints (sometimes). Alas, you can no longer use the same computer password for everything. Even if you try, the name of your dog or your child's birth-year doesn't have enough letters or numbers, not to mention cap and lower-case, or special-characters. And just how many variations of your cat's name can you remember? *Was it,* "*Mittens76*" or "*76Mittenz!*"? *Oh well, I will just write every account and password I use on a piece of paper and stick it under my keyboard. (After all, thumb-tacking them to my wall might be a little insecure.)*

2 ACCOUNTS, PASSWORDS AND SECURITY – UGH!

2.1 SECURITY OVERVIEW

2.1.1 Accounts and username (userid)

Account - Most computer applications or systems have accounts**.** An account holds information about you, and gives you access and privileges on the computer application or system.

Accounts usually have a:

> **Userid (username)** – A unique identifier to the account. Usually an email address or a short name that you pick
>
> **Profile** – The area that holds identifying information about who you are, as a user. This often includes information that might be used in the process of resetting passwords (such as smartphone number for receiving text messages, a set of security questions, etc.)
>
> **Password** – a set of characters known only by you, that allows you into the system or application.

2.1.2 Passwords – the good, the bad and the ugly

Like locks on a door, passwords are meant to keep applications and systems secure. And, they are meant to control the entry of humans. **Because passwords are meant for use by humans, they are the weakest link in the security of computer systems.**

> *Passwords need to be short, and simple enough for humans to remember.*
>
> *But…*
>
> *Passwords need to be long, and complex enough, to not be easily figured out by the millions of computer hacking programs that roam the computer world.*

The need to make passwords strong is the exact thing that makes them weak. Because people can't remember them, they have to write them down.

2.1.2.1 DISCUSSION

> *How many passwords do you have?*
>
> *How do you retain them? (Please don't share any of your secrets.)*

2.2 STRENGTHENING THE WEAK LINK - TWO-FACTOR AUTHENTICATION

Because of the inherent weakness of passwords, many computer applications now use *two-factor authentication*. **Two-factor authentication combines something you know, with something you have.**

> *With two-factor authentication, a password, by itself, is not enough. You also need something that you, and only you, have in your possession.*
>
> **Something you know**
>
> In most computer systems and applications, ***passwords*** **are something you** ***know***. As mentioned earlier, passwords are becoming longer and more complex, to keep someone else from finding them out.
>
> **Something you have**
>
> **Your computer, your smartphone or a removable thumb-drive are examples of something you *have*.** Another example is a *software key* (stored on one of these physical items).

2.2.1 DISCUSSION

> *You just got a new computer. You try to login to your online banking application. After entering your password, it says that it doesn't recognize your computer. What's going on?*
>
> *How does the banking application verify that the new computer actually belongs to you?*
>
> *An email and a text message are examples of the use of different channels of communication. How does the use of multiple communication channels help increase security?*

2.3 ACCOUNTS AND PASSWORDS – GETTING OR CHANGING ONE

As described in the first section, above, when you register for a computer application or smartphone app, you usually need to give them a unique name for organizing basic information about you: *Account, Username (Userid), Password*. This usually ties to your **email address**.

2.3.1 Registering

Part of the process for registering for an application, or changing your password or other information, almost always involves use of your email. *Many people have multiple email addresses, which adds to the confusion.So, make sure you can get to the right email.* Once you register, emails from that application will always come to that address.

Generally, you go through these steps:

- Give them your email address
- The application sends you an email to that address, which you must check.
- Often, there is a link in the email for you to complete the registration.
- Some applications have you choose a unique username (userid). Others use your email address as your username (userid).
- Most applications then make you choose a password. (This is often the most painful part. We will give some tips in a following section.)
- Some applications also make you answer some security questions that only you know the answers to -- these can be used in the future to make sure that *you* are, indeed, *you*.

2.3.1.1 DISCUSSION

What is the most difficult or confusing thing that you find, when registering for an application?

How about, when changing a password?

2.4 TIP – REMEMBERING STRONG PASSWORDS

Strong (i.e. long, complex, hard to remember) Passwords usually need:

- At least 8 characters
- Some caps, some lower-case
- One or more numbers
- One or more special-characters (maybe)

Here's some suggestions for coming up with a Strong Password.

2.4.1 Work it out on paper, first.

Figure it out before they start asking. If the app doesn't like something, change it on your paper, first. (Remember to destroy the paper when you are done.)

2.4.2 Song or phrase

Use the first-letters from a lyric from a song or other phrase in your head. Example:

It was the night before Christmas and all through the house

Using the first letters:

IwtnbCaatth

From the phrase, it's already long enough, and I already have some caps and lower-case letters.

So I could put a number in front and a special-character in back:

3IwtnbCaatth$

2.4.3 Characters from the keyboard

You can replace letters in your phrase with the related numbers (and/or special-characters) on the keyboard (pictured above). Example:

I am coming up with a password for an application called, “Verbatim.”

Verbatim

I will replace any letters from the *top row* of my keyboard with the closest number on the keyboard.

Use “1” instead of “A”

Use “3” instead of “E”

Use “4” instead of “R”

Use “5” instead of “T”

Use “8” instead of “I”

So, instead of *Verbatim*, I get:

V34b158m

(If I need, I can put-in a special-character at the beginning or end.)

Oops!

But be careful. This is useful if you always use the same keyboard or laptop. But it gets confusing if you use different keyboards or try it on a smartphone (as pictured above).

2.4.4 Use a keyboard pattern

Draw some kind of recognizable pattern on your keyboard, and then use the letters and numbers as the password. For example, let's say you create a pattern on your keyboard (as pictured above).

If you start this pattern at the number 3, it should be pretty easy for you to draw out the pattern each time. If it helps, you might even draw recognizable images or letters on top of the keyboard. In the case above, the password ends up as follows:

3waxcvgy7890-=

But be careful. This is useful if you always use the same keyboard or laptop. It even works on a smartphone. But it gets confusing if you use different keyboards or try it on a smartphone (as pictured above).

2.4.5 Your own pin for your passwords

Check out this article:

https://safeandsavvy.f-secure.com/2010/03/15/how-to-create-and-remember-strong-passwords/

2.5 HUMANS STILL NEED TO WRITE DOWN PASSWORDS

Much as you use any system to make it easier to remember Strong Passwords, THERE ARE JUST TOO MANY PASSORDS THAT YOU HAVE TO REMEMBER. If you aren't a human, you can probably remember them all.

But for the rest of us…

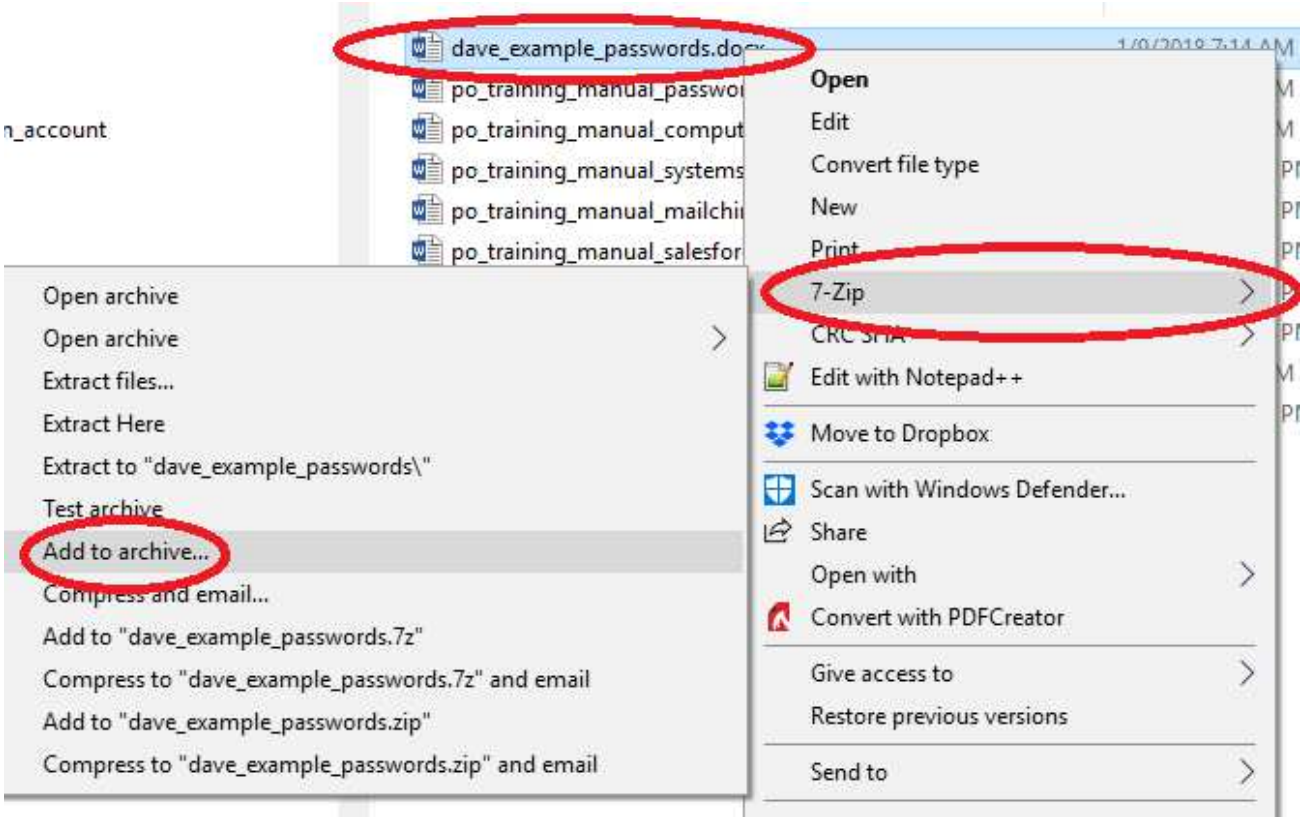
2.5.1 TIP – Encrypt your passwords

Whether you keep your passwords in a text file, a Microsoft Word document, or on a paper on your bulletin board, the goal should be to KEEP THEM IN A SAFE PLACE.

And this is almost impossible.

So, the next best thing is to ENCRYPT YOUR PASSWORDS, SO THAT YOU ONLY HAVE TO REMEMBER ONE PASSWORD – (the one needed to unencrypt your password list).

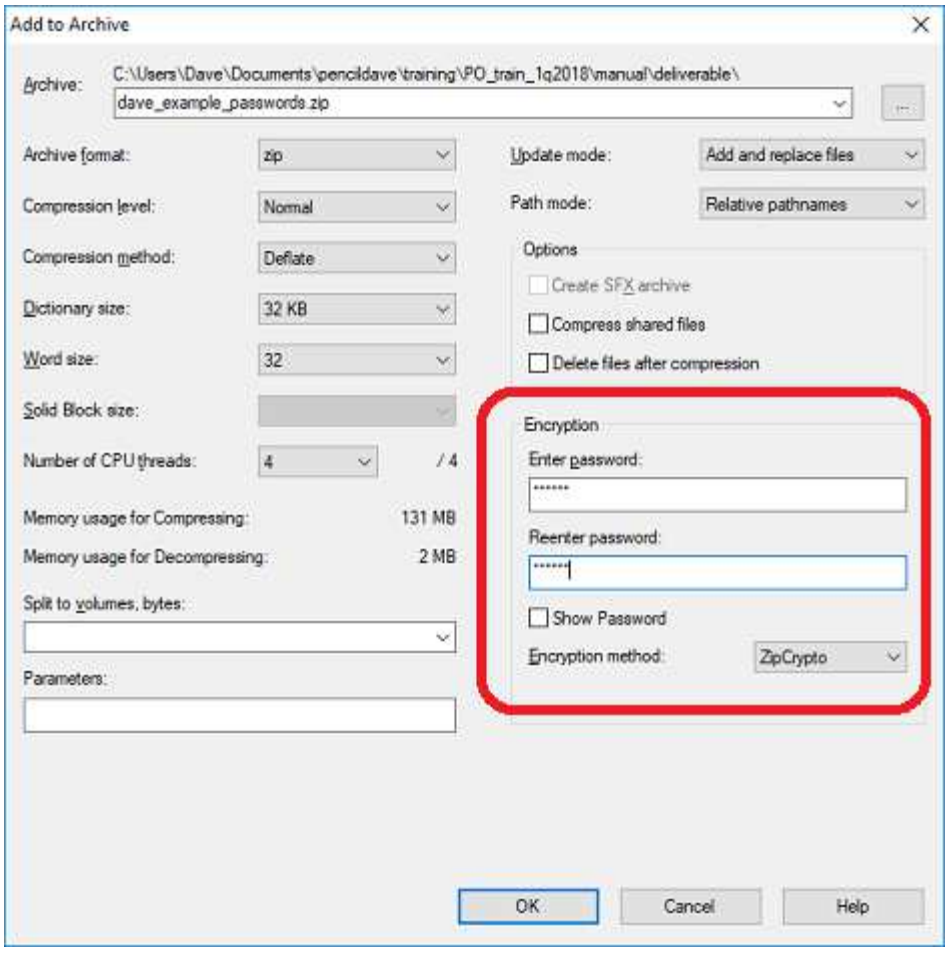
2.5.1.1 Encrypt using Winzip or 7-Zip



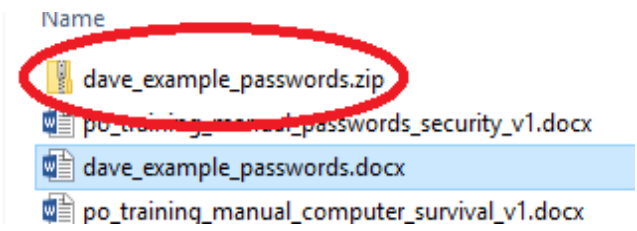
Using a "zip" program (like ***7-Zip*** – *which is free*, pictured above) offers a *minimum* level of security, since it is relatively easy for a computer hacker to crack an encrypted "zip" file. BUT MOST HUMANS DON'T KNOW HOW TO CRACK YOUR FILE, SO YOUR ARE RELATIVELY SAFE.

7-Zip is free software. You can get it here:

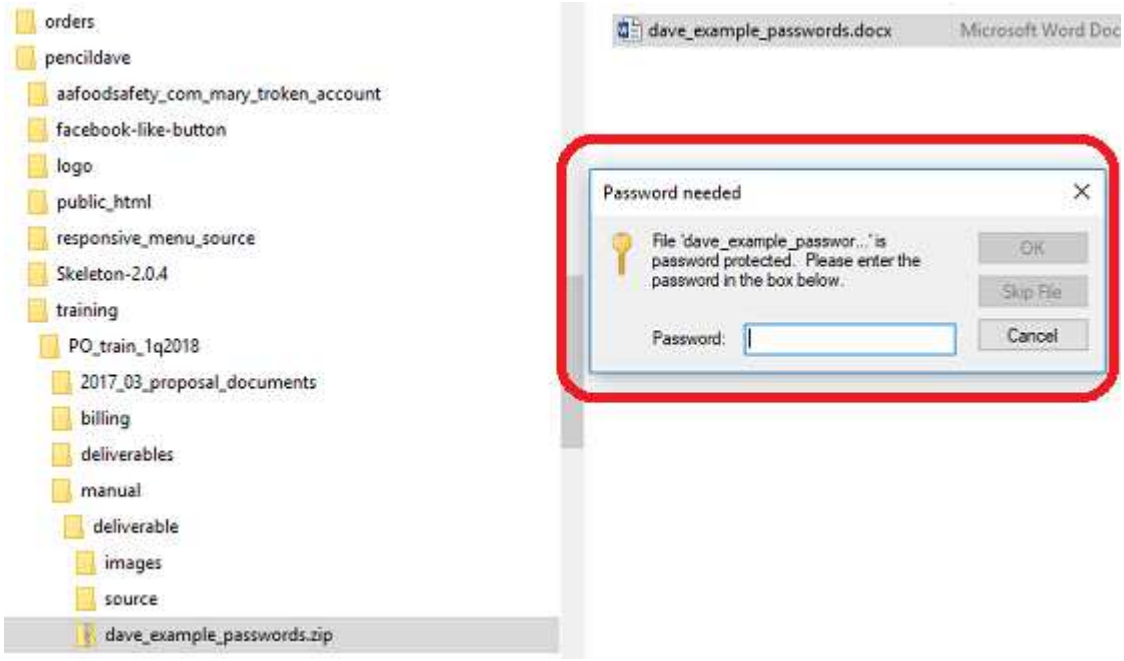
http://www.7-zip.org/



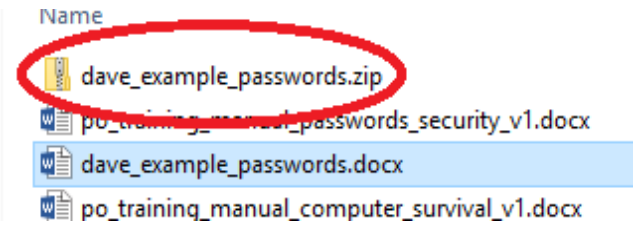
When I “zip” my file, I use encryption (i.e. give a password that I will use to unencrypt it later, in order to get into the document) – pictured above.



Newly created zip file, pictured above.



Now, when I double-click on the encrypted zip file, then on the document inside, I will need to enter my password, to read it (pictured above).



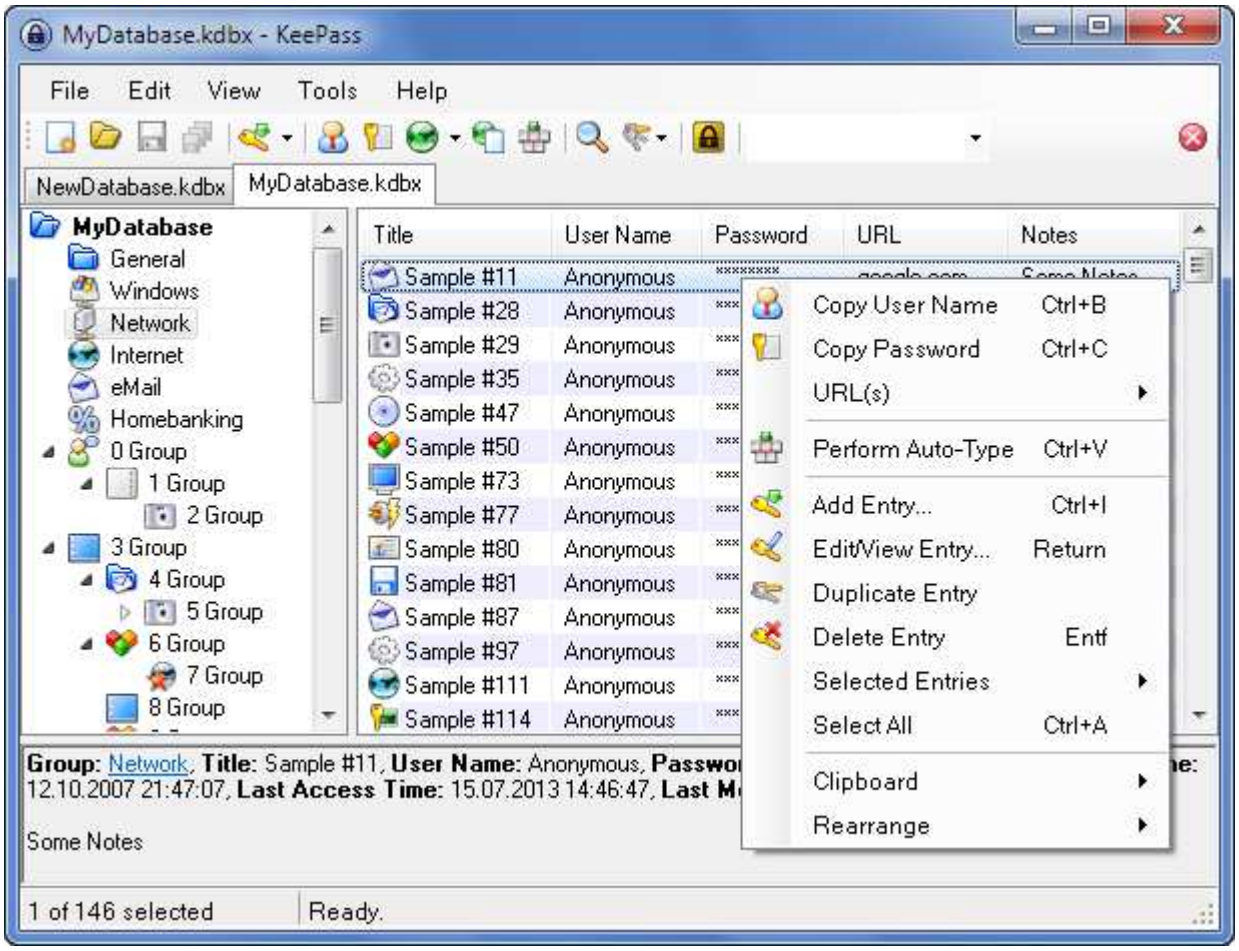
Remember to delete your original *passwords* document (the blue one, above). From now on, use your encrypted zip file (red circled file) of your passwords.

2.5.1.2 Use Password Manager software

Password Managers do essentially the same thing as we just did with Winzip or 7-Zip. Besides this, most allow you to synchronize your passwords database between devices (ex: your computer to your smarphone).

- **Advantage:** You can get at your passwords on your computer and/or your smartphone.
- **Advantage:** You can copy/paste passwords into fields (avoids complex typing)
- **Advantage:** Some programs automatically enter passwords into fields in your applications, so that you don't have to think about passwords at all.

- **Disadvantage:** When you synchronize, you are usually storing your encrypted file of passwords in the cloud. They are still encrypted, but the file is more readily available to the millions of hacking programs out there. (Note that, if you don't synchronize, you can avoid storing anything in the cloud.)



The Password Manager that I use is called KeePass (pictured above).

KeePass is free – you can get it here:

https://keepass.info/

2.5.1.3 DISCUSSION – Cloudy or Sunny?

Can you avoid the cloud?

2.6 SECURITY – GOLDEN RULES

2.6.1 Be judicious about giving away the keys to the kingdom

Every time you sign up for a new internet application and/or smartphone app, you give away more of your rights, and give away more and more personal information. This is usually plainly stated (or obtusely hidden) in the legalize that you breeze past before clicking on "yes."

It is almost impossible to use a computer or smartphone without giving up some personal information. For example – letting marketers (and who else??) know where you are at every moment of the day.

Social media apps (Facebook, Twitter, etc.) are meant to share your personal information. By nature, social media apps are less secure, even when you configure with various security controls.

Think about the ten apps that you just loaded on your smartphone. Are they worth what you gave up?

2.6.2 Passwords – update them regularly

We have heard this before.

But know that your passwords get broken on a regular basis. You have to concern yourself with, not only the random hacker, but with the millions of computer programs (called "bots") that constantly wander the internet, looking for weak spots to exploit.

Passwords can be broken, easily, by computer programs. It might be impossible, or at least take months, for a human to crack a password. But a computer program can crack a password, sometimes, in seconds, *especially if it is short and/or uses words that are in the dictionary*.

Strong passwords (the longer and more complex, the better) are more difficult for computer programs to crack. Instead of racing through combinations of twenty-four letters, or racing through all the words in a dictionary, a password that uses words NOT in the dictionary is much more secure. Especially, if it uses *strong passwords* – these are long passwords with combinations of *upper and lower-case letters* (now a program has to look through combinations of 48 characters), plus *numbers* (now it's 58 character combinations), special characters (*example: "!," "%," "(," "],"* *etc.*). You get the picture. *Yes, it's a pain!*

Change your passwords on a regular basis. Even strong passwords get broken in time. *If you haven't changed a password in over a year, assume that it has already been hacked.* Your only defense is to change passwords regularly.

What will hurt the most if it gets broken into? If someone breaks-in, what applications allow them to start spending your money? **Change passwords on these apps first.**

2.6.3 Sensitive information that hackers love

- Social Security Numbers
- Credit card numbers
- Tax id's
- Bank account numbers
- Life insurance account numbers
- Personal information (where you went to school, your mother's maiden name, the names of your pets, etc.)

The bad news – most of your personal information is already on the internet.

The good news – being vigilant on a regular basis (changing passwords, checking credit scores, etc.) reduces the chance of being hacked.

2.6.4 Email is very insecure

Don't send sensitive information over email. Even though email may *look* secure ("https//…," or the "lock" icon in your browser), EMAIL IS NOT SECURE. It is beyond the scope of this training to go through all the insecure points at which your emails can get hacked, or are already being scanned by various parties.

Even when you aren't currently using email, your personal information in past emails is available to others. This applies event to emails that you have already deleted.

For example, most people use email as a sort of file system or archive. This archive is stored on servers maintained by large services (gmail, yahoo, etc.). When you registered for email account, you gave these parties certain rights to scan your emails, even when they are sitting on servers. These emails are regularly backed up and stored by the email service. So even emails that you have recently deleted are likely to still be stored on backups, and available for scanning under certain circumstances.

The bottom line: if you don't want someone to know something, don't put it in an email. If your tax accountant or banking representative asks you for your social security number, don't email it to them. Even if they tell you that their email is secure, it is not. **If you can't give them sensitive information face-to-face then regular mail, or possibly fax might be an option.**

2.6.5 Firewalls, virus / spyware checker must be up-to-date

Computer and/or smartphone viruses and/or spyware are annoying, to say the least. They may generate unwanted pop-ups, advertisements, etc. They may make your computer or smartphone act erratically and/or often slow-down its performance. They are often difficult to remove, requiring a professional to get involved. Sometimes, they even require re-installing the operating system and software to the state that it was when it came from the factory.

PC's with Microsoft Windows are especially vulnerable. But any computer or smartphone, even those running Linux and/or Mac's and Apple devices can get viruses.

> *Many viruses and/or spyware can get installed on your computer and run without your being aware.*
>
> *Many viruses and/or spyware gather sensitive information and may transmit it to hackers.*
>
> *Most smartphones and computers are constantly, or at least occasionally connected to the internet, the main source for viruses and spyware.*
>
> *Even when your device is not connected to the internet, it can be vulnerable to a virus or spyware (i.e. when you install an application or read a DVD, CD, or thumb-drive.)*

Your protection against viruses and spyware:

A **firewall** – Most operating systems at the base of all computers and smartphones have some sort of firewall running. A firewall analyzes information coming into and/or being sent from your device. It also protects against intrusions by unwanted parties (for instance, the millions of computer hacker programs and "bots" that constantly try to gain access to your computer).

Virus checker – Virus checking software analyzes computer and smartphone application usage for *low-level patterns* that betray viruses that might be hidden in something that you invited onto your device (such as a link that you clicked on, a program or app that you installed, etc.). Virus checkers block the viruses from executing, as well as try to remove any viruses that might already be there.

Spyware checker – Spyware is a type of virus that is usually related to annoying adds and pop-ups. Spyware is often more difficult to remove than viruses.

Most security packages check for both viruses and spyware as part of the same package.

> **Make sure the software is set to update itself (with updated pattern files for new viruses and spyware) daily.**
>
> **TIP:** *When you have a virus/spyware checker correctly setup, leaving your computer running, and hooked to the internet is often better than turning it off and on. Set the software to update itself at night.*
>
> **TIP:** *Installing multiple virus and/or spyware checking programs is BAD, and weakens their ability.* ***Only install one virus/spyware checker.***
>
> **TIP:** *If you aren't sure about the protections against viruses and/or spyware on your device, have a computer geek take a look. (But bring cookies or beer – he or she is usually swamped with people with requests about virus problems.)*

2.6.6 Phishing emails, links and trojans

You have probably experienced **Phishing emails**. They are emails that look legitimate, but come from hackers. They are usually trying to get you to reveal personal information and/or click on a link. They can also be related to fake websites that look like legitimate ones (for example, your online banking website or credit card company website).

Phishing emails and fake websites, that imitate legitimate companies, are getting more insidious and harder to recognize.

Clicking on links in phishing emails and related fake websites are a popular way for hackers to install **trojans** (programs that look legitimate but install viruses) or compromise your computer in some other way.

Basic tips regarding phishing emails:

> ***Some phishing emails look like they came from someone that you know. A friend's compromised computer may be sending bogus emails from them, without their being aware.***
>
> ***Many phishing emails come from foreign hackers. They often contain spelling errors, grammar mistakes and/or awkward expressions.***
>
> ***If an email asks for sensitive information, such as a credit card number (or clicking on a link to update credit card information), don't do it. Just delete the email.***
>
> ***Some phishing emails try to look important. They might say that your account has just expired at your email carrier some other service. Or they might tell you that you need to an account or password. They try to get you to click on a link to do this.***
>
> ***Never click an email link that claims to go to a known company or provider, even if it looks legitimate. Always open a new browser session and go to the company or provider separately. Then login from there.***
>
> ***Trust your gut – If you suspect an email as being bogus, there is a good chance that it is. Don't click on any links. Just delete it.***

There are many articles for tips about phishing emails. Here are just a few links. [Dave??]

2.6.7 Prioritize security tasks

Concentrate your security efforts first on applications and systems that would cause the most pain if they happened to get compromised.

> *Use strong passwords and two-factor authentication for these apps.*
>
> *But remember that even the strongest security can always be broken.*

If you don't want to live with these realities, maybe you shouldn't use the system or app.
