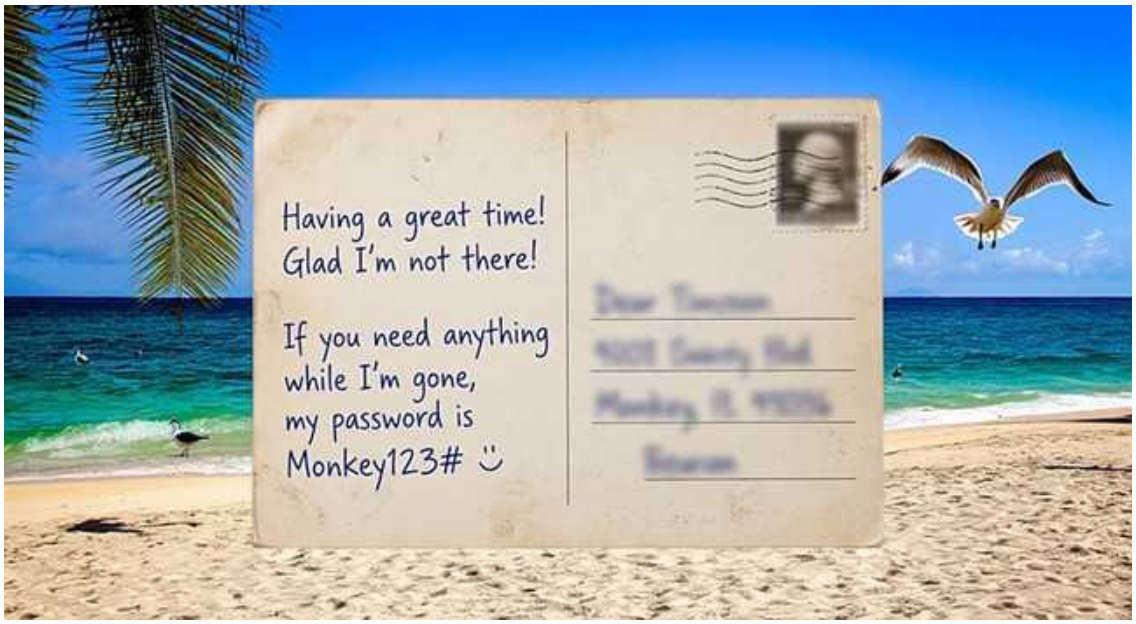
Science Translations
Established 1990
PC410.COM™
PC Updater News




## Don't Email Passwords!

Just a reminder: Emails are a relay system. The pathway between sender and recipient leads through a few or maybe a dozen other servers. The connections between each server is (generally) encrypted individually, but the text of your message is open and readable on any one of those relays, which are mostly secure, but not always safe. Internet message routing is really just ‘send it in the general direction,’ repeated until it arrives at the right place. That’s good–it routes around outages. And that’s bad–it’s security designed for the 1980's.

So don’t send passwords, credit card numbers, tax or medical information, or anything that should be secure through email. If you would not write it on a post card, don’t email it.

There are ways around that if you need them; ask me about secure web portals or secure email systems. (The one that's popular for financial work is 'Smarsh.')

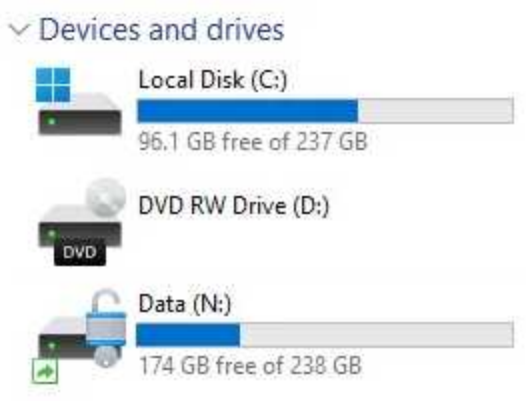

## Credential Stuffing

Defined: When a hacker collects one of your passwords, they try it everywhere. At the top 50 banks, and the most-popular online shopping sites, and on social media. Anywhere that lets them send emails, buy gift cards, or post messages is useful. And there are services that automate those attempts. If your passwords everywhere are all the same password, credential stuffing will create a very large mess when your one and only password is collected by malware. Use different passwords on every site, always.

To take more precautions against 'stuffing' attacks, use different user names everwhere as well, or at least on the important sites: banks, and any other site holding your credit card information.

## Is BitLocker Running? Back Up the Recovery Key!

BitLocker is the Microsoft brand of Windows drive encryption. Just in case your computer is stolen, or the system crashes beyond recovery, it prevents anyone who has physical control of your computer or drive from reading your files. It’s pretty good at that; getting file off a BitLocker drive is effectively impossible. A password on the login does not do that; I can get around that in around 10 minutes. However, this does not mean I’m encouraging the use of BitLocker; it’s not the best product in the category, and it can and does fail, and can lock you out of your files, permanently. And for a computer like a server that is always on, BitLocker gives you no protection against file copying; it’s only useful if the computer is off. A great lock that’s sitting open doesn't do anything.




The problem right now is that BitLocker is a feature of Windows 'Pro' versions and above. It's not officially part of Windows Home. And yet, there it is, **on by default on many major brands of laptops** and pre-configured desktop computers. Look at the drive image above. If any drive letter shows that padlock, the computer is running BitLocker. It's probably set to unlock the drive automatically during boot, without the password. That's done, silently, by saving the password in the TPM. That's the 'Trusted Platform Module' that was such a big deal during the Windows 10 to 11 transition; it was required in order to upgrade. The TPM chip in the computer stores BitLocker information, and also has some features and a little bit of storage to hold passkeys for websites. The result of this is that many PC users have BitLocker turned on without knowing it.

This is important. If BitLocker is on, that padlock will show, always unlocked if it's on the C: drive, or possibly locked if it's on some other drive letter. You must know the password to unlock the drive to use it, or the recovery key to recover data from it if there is any hardware change to the system. That's not either/or and not password or recovery key; you must have both of those items. The key is a 48-digit number,  with hyphens.

**Basically, I'm asking every computer user to look in File Explorer for a padlock**. If there is a padlock, and you know your password, follow these instructions by Microsoft to recover your BitLocker recovery key from your online Microsoft account. Store it in multiple places, but not on your computer, as that's the same as locking keys inside a car.

**BitLocker Recovery Key Retrieval**
https://support.microsoft.com/en-us/windows/back-up-your-bitlocker-recovery-key-e63607b4-77fb-4ad3-8022-d6dc428fbd0d

A reminder: Your Microsoft account is based on an email you used to create it. It might not be the email address you use every day; if those instructions don't find a key that you can print and save, try your other email addresses. And the password to your Microsoft account is not the email password, unless the account is on a Microsoft domain, usually ending in @outlook.com or @hotmail.com.

Now, if you don't know EITHER the password or the key, and you're not locked out of the computer, but the open padlock is there, we can turn off BitLocker. If you want to use encryption, it can then be turned back on, with a known password and a stored recovery key. As always, call me for help with this if needed. Saving the recovery key is fast, and will prevent problems.

And of course, image backups of your computer should make unencrypted backups. Rely on physical locks to secure the drive holding your backups. Encryption is an important tool, but it has to be handled carefully.



**For computer help, call 410-871-2877**
**Missed a newsletter?** Back Issues

**Mailing address:**
Science Translations
PO Box 1735
Westminster, MD 21158-5735