Preview

Dumpster Diving

Very common way to get data from a company is what we call old school dumpster diving. Garbage picking is the practice of sifting through commercial or residential waste to find items that have been discarded by their owners, but that may prove useful to the garbage picker. Garbage picking may take place in dumpsters or in landfills. When in dumpsters, the practice is called dumpster diving in American English and skipping in British English.

Since dumpsters are usually located on private premises, divers may occasionally get in trouble for trespassing while dumpster diving, though the law is enforced with varying degrees of rigor. Some businesses may lock dumpsters to prevent pickers from congregating on their property, vandalism to their property, and to limit potential liability if a dumpster diver is injured while on their property.

Dumpster diving is often not prohibited by law. Abandonment of property is another principle of law that applies to recovering materials via dumpster diving.

Police searches of dumpsters, as well as similar methods, are also generally not considered violations; evidence seized in this way has been permitted in many criminal trials. The doctrine is not as well established in regards to civil litigation.

Companies run by private investigators specializing in dumpster diving have emerged as a result of the need for discreet, undetected retrieval of documents and evidence for civil and criminal trials. Private investigators have also written books on "P.I. technique" in which dumpster diving or its equivalent "wastebasket recovery" figures prominently.

If you can get into a dumpster it’s a great source of information you can find passwords written on paper you can find phone directories financial information. In the modern era of paper shredders, it’s a lot less common but those pieces of shredded paper put together lead to information a lot of patients and some tape goes a long way.

One thing I tell people is don’t throw all your important shredder trash into the same garbage pickup when I clip a credit card it 3 I will put 1 piece in each garbage pickup for the next three weeks.

When you're picking out a shredder don’t pick the cheap staples model that just shreds in one direction pick the shredder that does criss-cross and up and down the more way the documents get shredded the better. Pick a shredder as well that cut things into small pieces the smaller the pieces the better. It makes putting the document back together much harder.

One thing I see people do all the time is they will shred a document put throw their backup CDs in the garbage remember those are digital documents those CDs should be put through the shredder as well. Most shredders nowadays come with a document, credit card, and disk shredder.

When you're going through your closet and you pull out those floppy disks remember those still can be read. If you need to dispose of them get a good scissor and cut them up into pieces.

Hard Drives

One thing to remember when throwing away electronics don't just throw away the hard drive there is data on there that should be destroyed either remove the hard drive and hang onto it or use a disk erasing tool there are tons of free ones out there for you to use.

If you ever take your computer into service anywhere and they tell you the hard drive is bad and they're going to replace it always ask for the bad one back. At my computer business, I have made it a habit over the years to always return the hard drive to the customer. There are companies out there they can properly destroy the drives and they are very reasonable.

When it comes to your hard drive people do not realize how much of your data is on their most people will say to me

"I don't care if someone sees my pictures after I toss out the hard drive"

But it's not just your pictures or music that attackers can get let me give you an example. Let's say you bring your computer in for service and the computer is 10 years old (by the way for the love of every real pc tech in the world don't use Geek Squad). The PC is running let's say Windows 7 and the PC tech says that the system board on the unit is bad.

So, you decide that the new Lenovo Yoga looks like something you want, and you should buy why to invest $200 dollars in a 10-year-old PC with an operating system coming up on end of life in 2020. Now on the way out you decide well this PC is junk let me toss it into the dumpster by your job its useless anyway and there is nothing you need on it right. WRONG!

A skilled computer person with about 2 minutes and a screwdriver can take that hard drive out of that computer than when they get to where ever they are going put the drive into an old computer boot it into Windows.

So now the attacker/person is on your computer well let's start with social media which we talked about in the last chapter how many us for ease of use have Google Chrome

save our password, so we don't have to log in every time. We all have hit that save password button from time to time. So the attacker now opens your web browser and boom they are now login to your Facebook account. The same applies to your email or Amazon.

I know you are going to say "I don't care if they read my email."

Maybe you don't care if they read your email but what about what your email is connected to and what you use it for daily. You need to protect your email for the reason being most important sites like your banking if you hit the "Forgot Password" button it sends an email to you to reset your password.

So right their all because you tossed out an old not needed computer you have now had a security breach of your finances. This could all happen within an hour of you tossing away a computer.

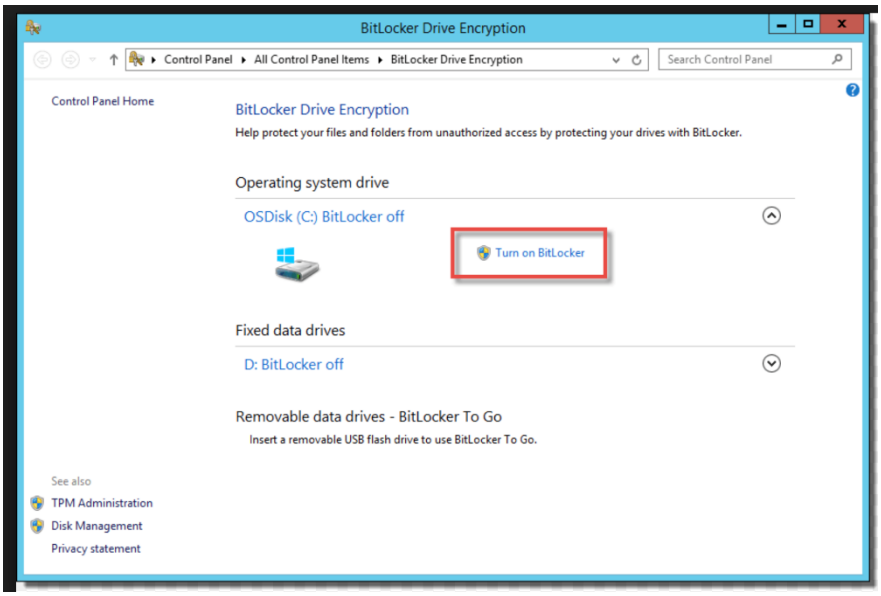
The other thing you could do to protect your computer is to encrypt the hard drive. Let me explain what exactly disk encryption is by definition. Disk encryption is a technology which protects information by converting it into an unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. It is used to prevent unauthorized access to data storage.

Now I know this seems very overwhelming but it's not. Both Windows and Mac have disk encryption as built-in options in this modern era of computing. If you are using a Chromebook, you are lucky you don't have to do anything the disk is always encrypted. Only the signed-in user can access their profile data. There is no administrator account that can access everything. So, your data on the Chromebook is always the safest.

Microsoft Windows has its own version of encryption called BitLocker.

To Enable Bitlocker just go to Control Panel – All Control Panel Items – BitLocker Drive Encryption. Just click Turn on BitLocker.

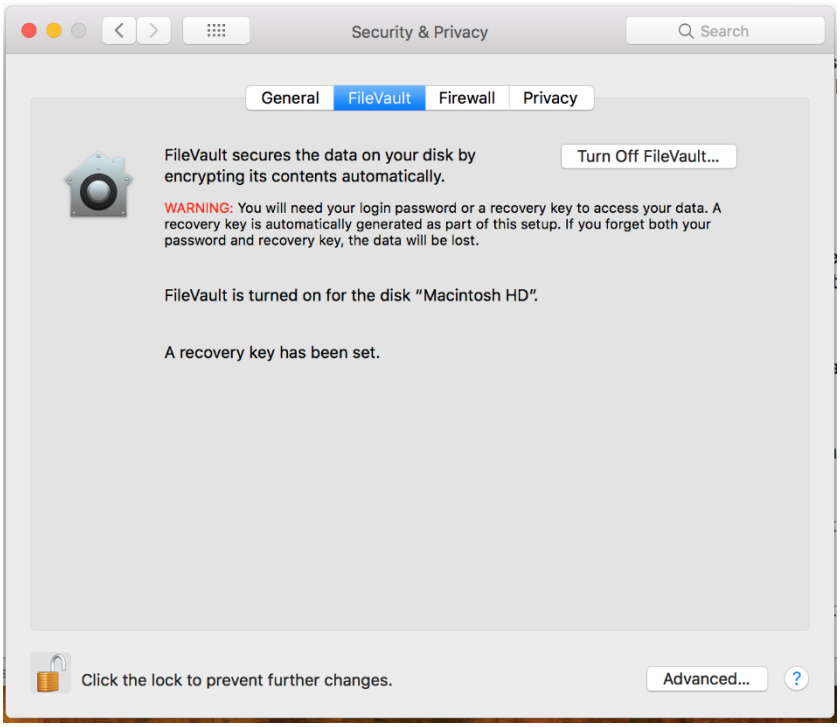
Follow the onscreen instructions they are easy



On a Mac, it's easy as well and with the integration of Apple iCloud its easier than ever to turn on Apple version of drive encryption called FileVault.

Just click on System Preferences – Security and Privacy - Click On The FileVault Tab – Click Turn On File Vault

You will then be asked for your iCloud account info and that's about it



Personally, I like to use a third-party tool called Symantec PGP Full Disk Encryption as it's a third-party tool and the inventor of PGP Encryption Phil Zimmermann actually works for Symantec. Zimmermann is the creator of Pretty Good Privacy (PGP), the most widely used encryption protocol in the world. Symantec PGP Full Disk Encryption will be overkill for most but you do get much more options then you do with Microsoft or Apple. But for just the average user the built options are more than secure enough.

Cell Phones

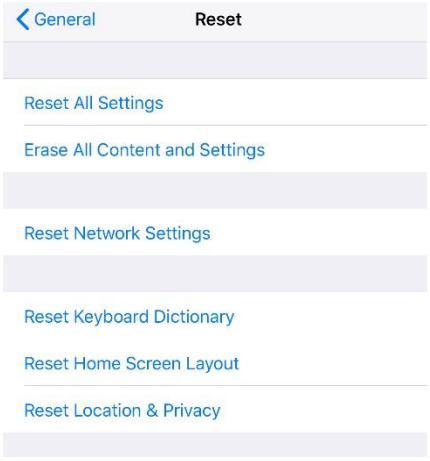
The same thinking with hard drives applies to cell phones. Cell phones should always be reset to factory defaults before giving it to a friend or giving it back to the company in exchange for a new one.

If you need to reset an iPhone this can be done in the

Touching the Settings Gear

Going Into the General Settings

Touching Reset



If you are getting rid of the phone tap Erase All Content and Settings

On Android, all the phone app layouts are a little different but you should find it in

In the Settings menu, find Backup & reset, then tap Factory data reset and Reset phone.

If you are a small business owner or someone who is worried about phone theft and the data on it there are many apps out there that allow for remote wiping of the phone.

Another very important thing to consider if you have important data on your phone is a passcode or biometric lock to allow for your device to be safe in the case of theft. Majority of people actually never put a passcode on their phone.

All iPhone and Android phones come with biometric scanners and with the popularity of iPhone it's only a few years till until FaceID is on all devices.

Laptops come with fingerprint scanners I strongly recommend if you have a fingerprint scanner on your laptop set up more than one finger encase you get a cut, crack or lose the finger you use. There should be as well an option for a password which I would recommend in the case of an emergency.

Most cell phone users never bother to think about their phone backups if your computer gets hacked and your cell phone backup is stolen someone can then use that backup to restore that backup to another phone to get your data.

One thing I have many times on the news is people get their email or Facebook accounts hacked because of their security questions. Let me explain when you set up a new email account or iPhone anything with a password they always ask you to set up security questions.

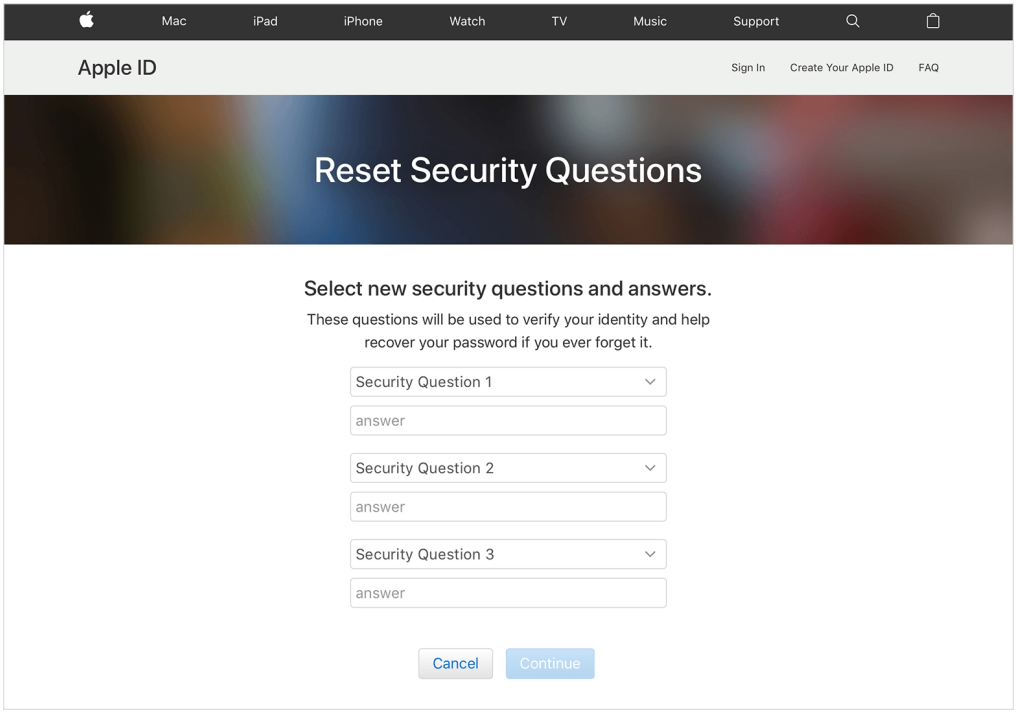
The issue with these questions is this if you pick something that everyone knows it can be easy to hack. For example mother maiden name I have seen so many people get burned with this question because when you apply for a marriage license they collect this information. If someone really wants to get into your account they just have to look up your marriage license. Friends that's another issue how many of your friends have access to that information.

Another question where people get hacked on a favorite sports team. How easy is it to check out your Facebook page to look for you at a game or to find the logo of the team someone where on the page.

The most common issue is the pet's name that's an easy one for almost anyone to find out especially close friends or family. There was a story about a celebrity a while back that got her Twitter hacked because she used the name of favorite pet question.

CNN – "In 2005, hackers logged into Paris Hilton's phone and stole photos of her, according to Mikko Hypponen, chief research officer at the F-Secure computer security company. Those hackers reportedly were able to break into Hilton's phone by correctly guessing the not-so-secret answer to her security question, which was "Tinkerbell," the name of her pet Chihuahua"

The safest way to deal with security questions is to both write down different answers then the real ones and keep them somewhere if you ever need to change your password. Apple has a nice idea they have three questions and ask you two of the three to see if you are who you are. Not the most secure way but better than just 1 single question.



When it comes to email addresses this something you really need to protect. Your main email address is the most important thing to protect. Remember your email address is used for your banking, ordering online and is pretty much your lifeblood online. If you forget your password to a site you will use your email address to have the new password sent to login. One thing you need to be careful about is if you see a lot of

password requests coming to your email address that's a sign that someone may be trying to hack your account for that website.

Spam & Phishing E-Mails

One thing to be careful about is if you are getting emails from sites you have never used or sometimes douses that could be a phishing email. Phishing emails are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your university, your Internet service provider, your bank). These messages usually direct you to a spoofed or fake website or otherwise get you to divulge private information (e.g., passphrase, credit card, or other account updates). The perpetrators then use this private information to commit identity theft.

Another thing to be careful when using your email is spam. Spam email is a form of commercial advertising which is economically viable because email is a very cost-effective medium for the sender. If just a fraction of the recipients of a spam message purchase the advertised product, the spammers are making money and the spam problem is perpetuated.

Spammers harvest recipient addresses from publicly accessible sources, use programs to collect addresses on the web, and simply use dictionaries to make automated guesses at common usernames at a given domain.

Spam is increasingly sent from computers infected by computer viruses. Virus-makers and spammers are combining their efforts to compromise innocent computer users' systems and converting them into spam-sending "drones" or "zombies". These malicious programs spread rapidly and generate massive amounts of spam pretending to be sent from legitimate addresses.

Spammers using specially designed software to generate false email headers and from addresses. Several email users have been affected by falsified messages claiming to be from the service's administrators, stating that users' account is closed and require some action by the user to be reopened. Such messages often contain viruses and should be ignored or deleted.

The general rule of thumb is if an email is in your spam folder it's probably junk and should just be deleted. Programs like Norton, McAfee and AVG scan incoming emails when you are using an email client like Outlook or Thunderbird but when using email online like in Chrome or Firefox the software can't protect for the safest email experience I recommend using a client with a good antivirus.

When hijackers succeed in sending spam via an email service, it can be temporarily blocked by other services and private domains who try to protect themselves. It's important that email users protect their own account with strong passwords to prevent their account from being hijacked. It's important for all computer owners to install and

maintain anti-virus software to avoid having their computer infected and possibly become a source of spam without their knowing.

One thing to be very careful about is closing an email account. I know a lot of people are going to say what the danger in deleting an old email account is. There can be a lot of problems with closing an old email. To start with an email address like @gmail, @yahoo.com, @outlook.com and may other are they are recycled emails. If I created an email account today on Yahoo and deleted it you could get that email if you wanted in 60 days. This is not a problem for an email account that was hardly ever used but what if you delete that email account and someone gets it and it was tied to an old credit card or old friends that may send you an email it would be very easy for the hacker to scam a friend for money or get a new credit card sent to a P.O. Box cause they are the owner of the email address on file.

The other thing to be very concerned about is old social media accounts. Believe it or not, you can still get into your Myspace Account if you really want to and look up old pictures it's still around. I bet if you really wanted to you could even get into your old ICQ account that's still around as well if you could remember your original number. My point is these old accounts can still be out there. Now granted these old accounts are not tied to anything but what about an old Facebook, Twitter, Amazon or Gmail account.

Many people over the years have said to me well I don't use that old Facebook account after my X and I broke up I opened a new one. Which might be a great idea but that old account is still sitting out there with pictures, information and verified by Facebook. What if someone were to get the password to that old account and send out a virus or spyware to those people still on your contact list.

What if that old Facebook account is tied to something like a login to a website? Even worse what if that old Amazon account still has an old credit card on file even if it's out data information do you still want attackers to access that information.

My point is just because you never touch an old account does not mean it's closed or deleted. Please be careful with how you dispose of sensitive information despite if it's electronic or on paper.