

Loose Data - What can it hurt?

We've all heard the saying "Loose lips sink ships" about careless talk that could reveal private or confidential information that could be used and harm others.

In today's world, we're aware of how important it is to keep private or confidential information secure, whether our customers' data at work or our own personal data at home. It's about more than not being careless about what we say around others. It's about not being "loose" with what private or confidential data we have control of and protecting access to it.

At work, we have policies and requirements about how we collect, handle, store, and dispose of all data. But what about at home, where we feel safe and may be a bit more lax?

Here are some tips to consider for taking control of your loose data.

- First, **secure your home router** by giving it a strong passphrase and a name that does not tell others who you are, such as "the Collins Family" or "123 Parkview Lane."
- Having the **most current security software**, web browsers, and operating systems are some of the easiest ways to protect your data, so keep these updated on all your devices!



- You already have long passwords for each of your accounts, right? Be sure to **add Multi-Factor Authentication** for any of them that store or use your sensitive information!
- Take stock of **where you may be storing digital data**, including all USB drives and other backup devices. They're small and easy to set down or toss in a drawer and forget about, so be sure they're password protected!
- Sensitive digital data stored on all portable drives could be **consolidated** into one place, making it easier to secure it.
- **Create a plan** for what data and records you need to keep and for how long (both digital and physical). Then permanently and securely dispose of all old or unnecessary records and data no longer required.
- **Securely dispose of any old devices**, including hard drives, laptops, tablets, copy machines, fax machines, etc. Make sure all your data has been wiped from them first.
- **Securely dispose of documents** with sensitive data so they can't be read by using a cross-cut shredder, burning, etc.
- And finally, know what data you have provided and is being stored in your apps and online services. Then, make sure your **security settings** are at the highest level for your comfort. It's your data - be as paranoid as you'd like.