**Data Security Checklist for Associations**

**1. Data Retention & Destruction Policy**

Have a policy in place that sets the retention schedule for your data.

Be sure to include electronic records.

Lock down all member data, paper included.

Inventory what you have, scale down when possible and properly dispose per the schedule you have set.

**2. Lock and Protect Your Devices**

Remember, something as simple as screen lock (on a Windows machine it is Windows key and the letter L) when you walk away from your PC/laptop even for a moment.

Be sure you have password protected your smartphones and tablets and if Touch ID is available, use it.

For iPhones and iPads, install Find My Phone so if you set your phone down and cannot remember where, you can find it quickly.

**3. Inventory Who Has Access to What**

For association employees create a list of what systems/data they have access to so when they leave you have a record of which user information you need to shut down and turn off. Don't forget keys/key fobs and physical access as well.

If you have vendors or consultants who have access to your data, be sure to have a list of those as well and what they have access to so when a project is complete you can turn off their access.

**4. Include Data Protection in Contracts & Service Agreements**

Be sure any contracts you have with vendors and service suppliers include language that protects your data.

Examples would be email companies who do blast emails for you, companies that create mailings for you based on your member data, vendors who provide and host systems for you that create registrations, Calls to Action, etc, where an outside entity has access to your member data.

Involve your attorneys to make sure the agreement spells out exactly how the data can be used and your protection against any misuse.

**5. Data Privacy Policy**

Develop a data privacy policy and have it reviewed by your attorney and approved by your Board of Directors.

Publish the policy where your members can access it as well as distribute it out to your members.

In November 2007, NAR's Board of Directors approved the following motion:

All POEs be encouraged to adopt a Privacy and Security Policy, using NAR's Privacy Policy as a template, or their own, and that it be visible and accessible so members know their information is secure. POEs that have a specific or a more restrictive local policy may adopt their own.

You can find NAR's Privacy Policy at the bottom of the realtor.org (nar.realtor) home page.

**6. Keep the Personal Private**

Be aware of the personal information you release whether it is via social media, password use, etc.

We recommend that you do not use personal information when it comes to setting up access to business information such as the association's member data, the association's bank site, etc.

Hackers can often put together information from your personal social media, for example, and use that to break in to business systems as well if you mix the two.

Be careful when using a public wi-fi and consider protecting your association's systems with a VPN so you can connect more safely when out of the office.

**7. Passphrase, not Password and Password Vaults**

It takes one day to crack a password that simply contains alpha characters, even when some are in caps and it is a long password. It takes 10 centuries to crack a password that contains alpha, numeric, special characters, numbers and is longer than 8 characters.

Use a "passphrase" rather than a password. For example, take a favorite song or quote (that not everyone knows that about you) and using the first character of each word in the first line of the song or quote, substitute some numbers and special characters.

Consider using a password vault manager like LastPass or 1Password. You can store all your sites and passwords, setting them up as complicated, and then need to remember only the one password to your vault.

**8. Dispose of Office Equipment Safely**

If you still have a physical fax machine, consider replacing it with an electronic fax service. Incoming paper faxes, especially your members' data such as applications are very easy to 'walk out' with.

When getting a new smartphone, if you are not keeping the same number or SIM card, remove the SIM card and microwave it for a few seconds to completely erase it. And remember to erase your old phone.

USB drives can be taken out of their metal/plastic casing and shredded.

When replacing PCs and copiers, remove the hard drives and have them shredded.

**9. Resources**

Keep up to date with what is going on in the data security arena. You do not need to be a 'hacker expert', but you do want to be aware when something your association uses such as social media sites, banks, etc have been hacked so you can change passwords and check your data.

It is also useful to not only know 'what' but how something was hacked. The following are great resources to use to keep up to date.

Wikipedia keeps up to date with the latest data breaches and cyber attacks:

https://en.wikipedia.org/wiki/List\_of\_data\_breaches

https://en.wikipedia.org/wiki/List\_of\_cyber-attacks

"Data Breach Today" contains articles on the latest news in data security:

http://www.databreachtoday.com/news

**10. Common Sense**

Always the best defense.

When in doubt, pick up the phone if something seems 'fishy' about the request in the email.

Remember the protocols we use in person and apply the "what? wait…" to electronic communications as well.

You would not give out your credit card or bank information in a conversation when meeting someone in person, so do not do so electronically.

Would the sender of the email ask you to do the same thing if you were conversing in person?

There is no need to answer the security questions with the real information. 'Fake it' and be sure to store those fake answers in your password vault so you remember them.

Limit access to your member data. Does everyone in the office need to see all the data, see all the member applications, see all the bank statements, etc, to do their job?

Never leave your laptop/tablet/smartphone unattended, even for a few moments when you run up to the counter to get more napkins.

And remember, no one needs to know your mother's real maiden name except your mother.

 