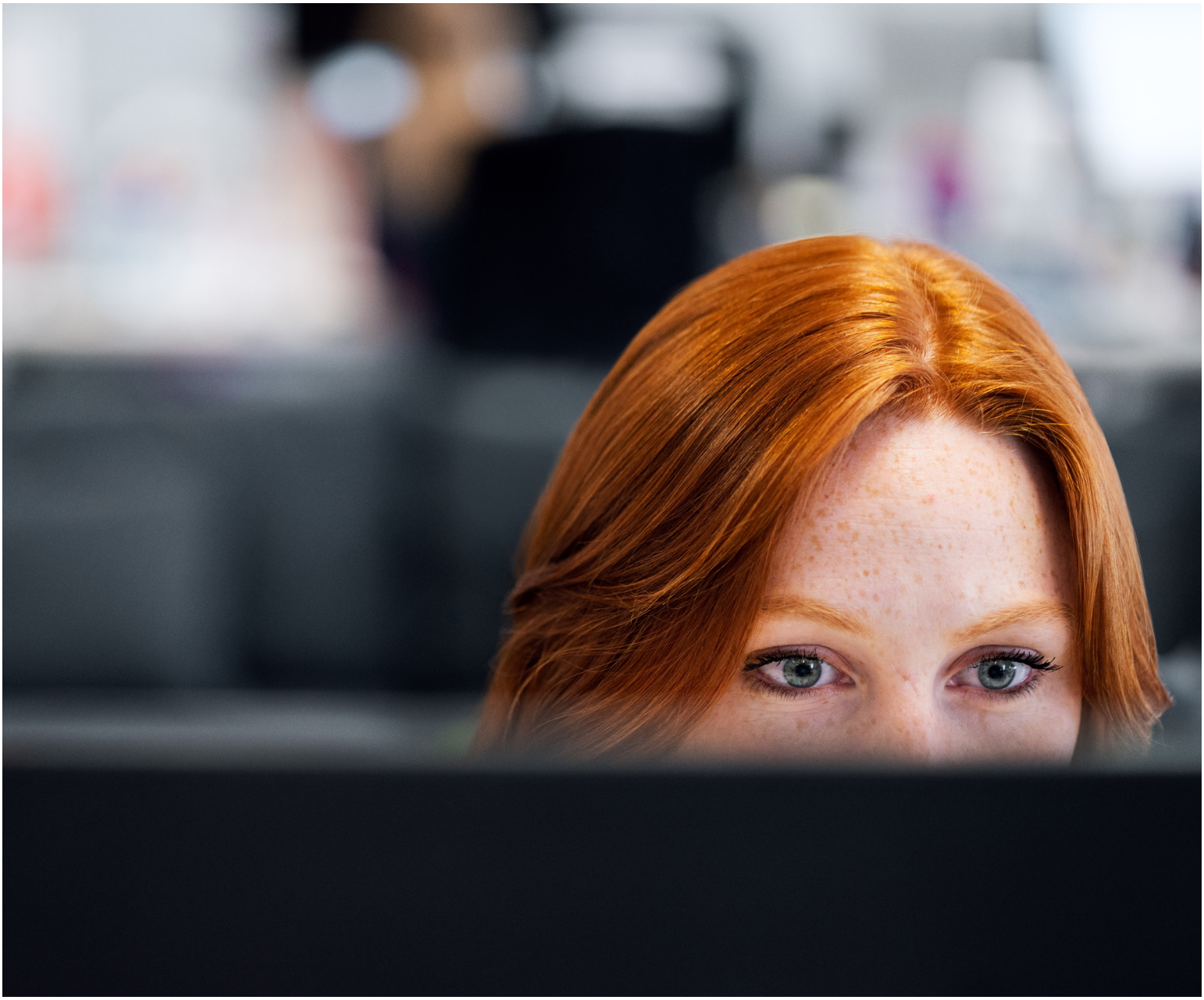
A FRAZER GUIDE

Cybersecurity for Your Funeral Home

A FREE EBOOK *by* FRAZER CONSULTANTS



When it comes to cyberattacks, everyone thinks they're safe. You may think "Why would they want my information?" or "I have nothing to hide." However, once a cyberattack happens to your funeral home, you'll realize how detrimental it can be to your business.

Hackers can ruin your important files and steal sensitive information, which may lead to you paying a hefty price. That's why it's important that your funeral home stays one step ahead. Getting a Secure Sockets Layer (SSL) Certificate, creating complicated passwords, and practicing email and WiFi safety are just a few ways you can keep your information secure.

This guide will go over ways you can stay on top of your funeral home's cybersecurity and avoid online threats.

Table of Contents

04

Importance of an SSL Certificate

06

Creating a Password

08

Email Safety

10

Keeping Your WiFi Secure

11

Backing up Your Data

13

Offline Risks

14

Conclusion

IMPORTANCE OF AN SSL CERTIFICATE

As hackers come up with new ways to steal sensitive information, an SSL certificate becomes increasingly necessary for your funeral home's website.

First, we should start with what exactly an SSL certificate is. An SSL — Secure Sockets Layer — certificate is a small data file that encrypts the data that's exchanged between your web server and browser.

When your data is encrypted, it's basically scrambled in a way that hackers cannot decipher. It only becomes legible again with the proper decryption key. This is important because it protects sensitive information that is entered online such as credit card information, social security numbers, and login credentials.

Knowing the Difference Between HTTP and HTTPS

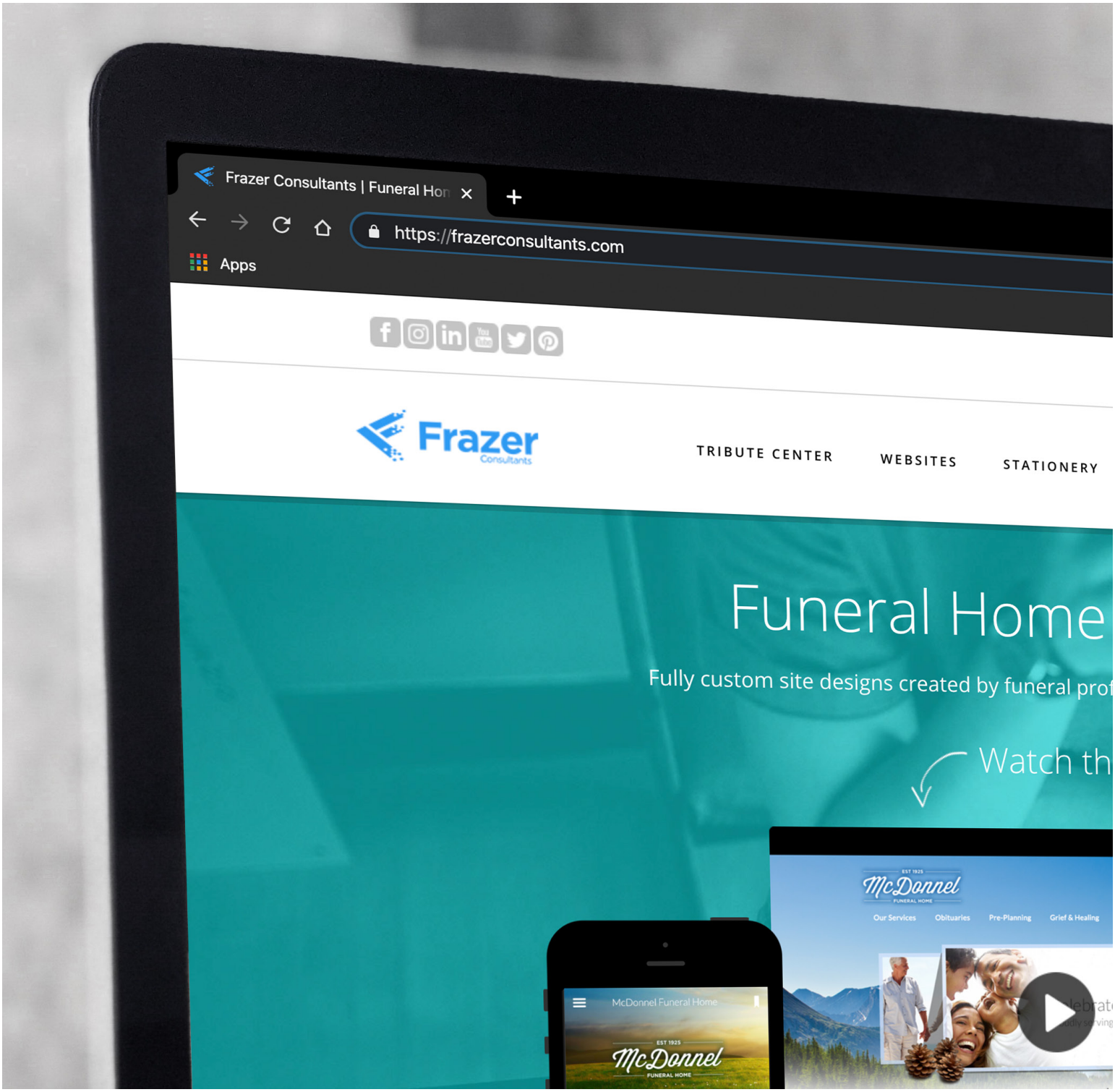
When you have an SSL certificate, HTTPS will go before your website's URL address. HTTP stands for hypertext transfer protocol. The "S" at the end stands for secure, so families will know that your website has a secure connection.

It's becoming the norm to have an SSL certificate for your website. Not only do customers expect it but so do search engines like Google. In fact, Google prefers HTTPS websites over HTTP websites which means having an SSL certificate will improve your search engine optimization (SEO) and your website will rank higher in search results.

As SSL certificates become expected, Google Chrome also will show families an alert when a website is not secure. This means that even less tech-savvy families will know that they should stay clear of unsecured websites.

Having Your Client Families' Best Interests in Mind

Besides helping your SEO and making your website more visible online, having a secure website helps your client families. When they enter payment information, they can feel at ease knowing that their information is safe.



A data breach makes your business look less credible and adds stress to families who are already coping with the loss of their loved one. With an SSL certificate, you can let your families know that they can trust you and your business practices.

All Frazer-powered websites are protected with SSL, so your families don't have to worry about hackers stealing any of their information — everything is safe and secure.

CREATING A PASSWORD

A strong password that is impossible to guess is key to protecting your funeral home's accounts and information.

One of the easiest ways to improve your cyber safety is to create a secure password. That means creating a password that no one else could ever guess. Because once hackers get into your personal accounts, they can begin to figure out ways to compromise even more of your personal information and data.

The Longer, the Better

Short passwords are a surefire way to get your account hacked. In fact, many websites require your passwords to be a certain length and have various characters, numbers, and capitalization when creating an account. Creating a long password makes it harder for others to guess what it is.

Don't Use Common Phrases

Phrases like "FuneralDirector1994" or anything that has your funeral home's name in it are not secure. Come up with a nonsensical phrase that only you could come up with. Avoid using your name, pet's name, spouse's or child's name, or any significant dates.

Jumbling up different characters, letters, and capitalizations also will make your password more secure. Password management softwares also can help you create a strong password. They automatically create and store your passwords for you.

Keep it Secret

For certain accounts, it's inevitable that you may need multiple employees to know the login information. That's okay, but make sure only people who absolutely need to know it have permission. Make it clear to your employees that passwords are not to be shared.

If you must write your password down, store it somewhere no one else will find it such as a locked safe. Also, be sure to change your password regularly, especially if it's known to multiple people. If an employee knows your passwords and leaves your firm, it's a good idea to change the passwords they might have known.

One Password Per Account

Many people are guilty of using the same or a similar password for all or many of their accounts. This is basically asking for hackers to break into all your accounts! Use a unique password for every account and don't use old passwords more than once.

EMAIL SAFETY

Spam and phishing are some of your biggest enemies when it comes to keeping your computer secure.

Hackers are getting more advanced in the ways they use email to get your personal information. That's why it's important to stay informed on ways you can protect yourself and your funeral home while using email.

Phishing

According to Wombat Security's 2019 State of the Phish Report, 83% of survey respondents experienced phishing attacks in 2018, which is up from 76% in 2017. Phishing is when hackers target you by email, phone call, or text message pretending to be from a legitimate institution (such as a bank or credit union). Their goal is to trick people into revealing personal information.

As hackers become more clever, their phishing emails begin to look more legitimate than what you imagine a spam email looking like. Oftentimes, they pose as HR representatives from your company or as tech support.

Phishing.org lays out a few common features of phishing emails. The first is they are often too good to be true. If the email is promising monetary gain, special deals, or prizes, it's most likely a phishing scam. Also, if there is a sense of urgency (ex. "Act now!") it's often best to flag it as spam and hit delete.

Hyperlinks and attachments are also things to be cautious of. Look for misspelling of links before deciding to click and never open an attachment from an unknown sender. Even if the sender's name is one you're familiar with, double-check their email address to be sure it's actually who they claim to be. If you receive an email from an unknown or unusual sender, chances are it's phishing.

Malware

Since phishing is an umbrella term for many cybercrimes, let's focus on malware. Malware is software that can wreak havoc on your computer, server, or computer network.

It's important to keep in mind that email is responsible for delivering 94% of malware, per the 2019 Verizon Data Breach Investigations Report. To stay safe from it, always be wary of URLs and attachments in emails. If you're ever unsure of a link or shared file from a coworker, ask them about it outside of email. Hackers can make it seem like their messages are coming from people in your contact list.

Also, to reiterate, never open a file from an unusual sender. Even if it looks like it's coming from your financial institution, it's important to double-check, especially if you are not expecting to receive files from them.

More Email Safety Tips

- Avoid sending sensitive information via email.
- Change your password frequently.
- Log out of your email when you're done using the computer.
- Be choosey about who you give your email to.
- Use a spam filter and anti-virus protection.

KEEPING YOUR WIFI SECURE

Did you know your WiFi could be vulnerable to hackers? It's unfortunate but very true.

When using public WiFi at places like a coffee shop, airport, or library, it's important to do things like using a VPN (virtual private network) or turning off sharing on your device. But did you know there also are security measures to take for your funeral home's WiFi?

Create a Secure Password

Foremost, it's crucial to have a password for your WiFi. Oftentimes routers will come with a password, but if you want it more secure, reset the password to a long, nonsensical phrase.

Keep up with Security Standards

Make sure your WiFi network is using the WPA security standard rather than the outdated WEP one. Also, changing the SSID (your network name) makes it harder for hackers to determine the make and model of your router, which makes it harder for them to break into your network.

Make a Guest Network

To accommodate families and guests, set up a separate guest network for them. This way, they won't have access to your internal network. Ask your provider how you can set up a separate internet connection with its own wireless access point. It's likely that your router already has the capability to run two separate WiFi networks at the same time.

Even with a guest network, still use a password that you can provide upon request. It's more secure for your guests than an open network.

Use a VPN and a Firewall

If a hacker does get into your network, a VPN will help maintain your privacy. Basically, a VPN encrypts your data which makes it private from others.

A firewall is another line of defense against cyberattacks. It's a security system that decides which network traffic is allowed in and out based on predetermined security rules.

BACKING UP YOUR DATA

If your data does become compromised, you will be thankful that you backed it up in a safe place.

Backing up your data is always a good idea. That way if your files become compromised or your computer unexpectedly crashes, you won't lose any important documents. Since this guide is all about cybersecurity, let's talk a little bit more about how hackers can hurt your data.

Many computer viruses affect your documents and files as they infiltrate your computer. Certain parts of your file may be unable to be read, or your file could be broken entirely. Sometimes within only a few hours of the cyberattack! That's why backing up your data makes these attacks less devastating to your business.

Store It in the Cloud

One way to keep your data safe is to back it up in a secure cloud. Basically, "the cloud" means your files are stored online through some kind of service. With your login credentials, you should be able to access your files on any device.

The benefit of using cloud computing services is that it's extremely unlikely your files will ever be lost. The cloud can't be broken or destroyed like a hard drive. If a cloud service were to go out of business, they would warn you to back up your files elsewhere. Also, they make it convenient for multiple employees to access and edit files from multiple devices.

Some of the most popular cloud computing services are iCloud, Google Drive, OneDrive, and Dropbox. Most offer a set amount of free storage and then charge for anything more.

When using a cloud computing service, it's important to keep in mind that hackers could try to access this data as well. Always practice good password safety as outlined earlier.

Physical Backup

There are many ways to back up data offline as well. One of the best ways to do it is using an external hard drive since they typically have more storage than other physical methods. Though most hard drives require you to plug them into your computer when backing data up, some are now wireless!

If you're looking for more portable ways to back up data, you could use a flash drive. Burning it to a CD, DVD, or Blu-ray disc also is an option as well. The device you use all depends on your personal preferences and needs.

Since you're working with many documents and a lot of paperwork, you're going to need a decent amount of backup storage. See how much data you currently have and think about how much that will increase in years to come.

OFFLINE RISKS

Cybersecurity attacks may not always come through email or account hacks. They can come from physical, offline threats.

Offline threats can be even more difficult to avoid. That's why it's important to keep these threats in mind.

Unknown USB Flash Drive

Never plug an unknown USB flash drive into your computer. It could be full of malware that can damage your funeral home's network and computers. When using your own flash drives, always be sure to label them and store them in a safe place.

Social Engineering

One form of phishing is social engineering. This tactic is when hackers use manipulation and deceit to trick you out of revealing your personal information.

A few ways this can be done is over the phone or in person. They will often pose as someone from the bank or a credit card agency needing your information. They will act with a sense of urgency, often making you believe that you need to confirm your personal information.

Establish a protocol for your employees when it comes to revealing personal information. You could always say you'll call them back and then find out if the number they are using is legitimate. You also can call the company they are claiming to be to confirm if they were the ones who called.

Limiting Access

Not everyone at your company necessarily needs access to all your accounts and documents. Decide who needs what in order to properly do their job. Also, never leave any personal information laying out — including sticky notes with login information. And never leave your computer logged into any accounts while you are away from it.

Conclusion

Knowing that all these cyber threats are out there may be overwhelming. However, by following the right precautions, it doesn't have to be! By taking the time to set up your funeral home's cybersecurity, you will be saving even more time and money in the long run.

ABOUT FRAZER CONSULTANTS

Frazer Consultants is a technology company that helps funeral professionals reimagine the funeral experience for their families.

866-372-9372 | info@frazerconsultants.com | www.frazerconsultants.com