bank prov.

Security Tips: Q & A's

How do you keep your Personal Information safe from an unsolicited call or email?

Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet, unless you've initiated the contact or know who you are dealing with. For example, if a company reaches out to you via email, claiming to have an account with you, don't click on links or open an attachment in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service.

Alternatively, call the customer service number listed on your account statement. Ask the company directly if they really did send the request. Similarly, if you receive a call, hang up or refuse to give out information, and then all the company using contact information you retrieve on your own, or have listed on documentation you have.

How do I create Complex Passwords for my online accounts? What is a Password Manager?

To create strong passwords, use variations on capitalization, numbers, punctuation, and always avoid names, places, and dictionary words. Try using a passphrase – take a sentence that is personal and memorable for you. Take the words from the sentence, then abbreviate and combine them in unique ways to form a password or switch out some of the letters from numbers and punctuations. Here are some examples:

- The first house I ever lived in was 200 First Street. Rent was $400 per month = TfhIeliw200FS.Rw$4pm
- Fly me to the moon = Fm32m00n
- Hard to Crack = H@rd2Cr@ck!
- To be or Not to be = 2B30rN0t2B3

Many people use very weak passwords and reuse them on different websites. How are you supposed to use strong, unique passwords on all the websites you use? The solution is a password manager. Password managers store your login information for all the websites you use and help you log into them automatically and there are a variety of password managers available. In addition, they give you the option to have them create a very long, complex and difficult to crack password automatically. Password Managers also encrypt your password database with a master password – the master password is the only one you must remember.

What is multi-factor authentication?

Multifactor authentication (MFA) is a security system that requires more than one method of authentication to verify a user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what a user knows (password), what a user has (security token) and what a user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Examples of MFA scenarios:

- Swiping a card and entering a PIN.
- Logging into a website and having to enter an additional one-time password (OTP) that the website's authentication server sends to your phone or email address.
- Attaching a USB hardware token to a desktop that generates a one-time passcode and using the one-time passcode to log into a VPN client.

Malicious websites and emails with links or attachments can seem enticing, how do I know what is safe and what is not?

Only click it if you're expecting it. For example, if you just ordered something from Amazon, it would be reasonable to receive and click on the shipment tracking link in the email they send you - just make sure it's exactly what you're expecting. If you get a tracking link that you were not expecting, or for a product you don't recognize, delete the email right away. In addition, you just signed up for a new online account. If they send you a link to confirm your email address, it would make sense to click on it, completing the process you have started. As always, just make sure it's exactly what you were expecting, and you specifically remember requesting it.

In the case of your bank or other institution, go to the website directly and log in. Type the address into the browser manually or click on your saved bookmark. By doing this, you can see if there is something that needs taken care of without the risk of ending up on a phishing site. In a case where your friend emails you, chances are that they copied/pasted the link into the message, which means you can see the full address. You can just copy/paste the same address into the browser yourself without clicking anything. Of course, before doing that, make sure you recognize the website and it's not misspelled.

How do you back up your data?

Backing up files can protect against accidental loss of user data, database corruption, hardware failures, and even natural disasters. The process of backing up is the creation of a secondary copy that it is available for restoration after a data loss event. The most basic and complete type of backup is a full backup. As it implies, this process makes a copy of all data to another set of media: tape, disk, DVD or CD.

Always remember:

There are going to be things that a small business owner can't do alone. For very important contracts, you get outside legal advice. For annual and quarterly financials, you have an accountant. The same approach should go for security expertise. When you need to test a site to make sure it's web-safe, or conduct a risk assessment, it's money well spent, if you don't have the expertise to do it yourself.