bankprov.

security tips and tricks.

Protecting Yourself and Your Business

phishing scams.

Every year, people lose millions of dollars, as well as, their personal information to tax scams. Criminals can use the regular mail, phone, or email to setup individuals and businesses a like so it's important to stay up-to-date on current scams and know how to spot them.

how the scams works.

Criminals have a number of tax-related tricks when it comes to stealing money and/or sensitive information. Here are a few examples of sophisticated tax scams that have taken place:

- Scammers send emails posing as tax service companies by spoofing emails and using stolen logos. Once you respond to the email with personal data or tax information, they pocket your hard-earned money;
- Similar to the scam above, criminals send look-alike emails containing hyperlinks that lead you to malicious websites or fake PDF attachments that download malware or viruses to your computer;
- Scammers make phone calls posing as an IRS representative, claiming that you owe money that must be paid immediately. The callers typically threaten arrests, deportation, or suspension of a business or driver's license.

Keep in mind, these are only a few examples—criminals are constantly coming up with new ways to fool their targets.

how to recognize a scam.

Keep the following in mind, especially during tax season:

- The IRS will always mail a bill or notice before calling you about taxes owed;
- The IRS will never ask for credit or debit card numbers over the phone;
- The IRS will never immediately threaten to arrest you for not paying taxes owed;
- The IRS will always offer the opportunity to question or appeal the amount owed before demanding your payment;
- The IRS does not use emails or text messages to discuss personal tax matters, such as taxes owed or tax refunds.

Only share sensitive data over email when there is no other alternative and you are certain the recipient is valid.

If you believe you've fallen victim to a phishing scam, contact the Treasury Inspector General for Tax Administration to report it. Visit treasury.gov/tigta/contact_report_scam.shtml or call 800-366-4484. You can also report a scam to the Federal Trade Commission by visiting reportfraud.ftc.gov.

If you've received an unsolicited email claiming to be from the IRS, or an IRS related component like the Electronic Federal Tax Payment System, contact the IRS using phishing@irs.gov. The IRS does not initiate contact with taxpayers by email, text messages, or social media channels when requesting personal or financial information.

social engineering.

Social Engineers are hackers who exploit the one weakness that is found in every organization: the human. Using a variety of tools, including phone calls, social media, email and devices, these engineers trick people into offering them access to sensitive information.

three common attack types.

Phishing: Phishing scams are the most common type of social engineering attacks used today. Phishing attempts are performed to obtain personal information, such as, name, address, social security number, or account number. Often, shorter or embedded links that appear legitimate are used to redirect a user to a malicious website. At times, threats or a sense of urgency may be used to manipulate the user into action on the request.

Some phishing emails are poorly written, oftentimes exhibiting spelling and grammar errors, but are still capable of directing victims to a fake website or forms where they can steal user login credentials and other personal information.

Pretexting: With pretexting, attackers focus on creating a good angle, fabricating a realistic scenario, that they can use to steal personal information. These types of attacks commonly take the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity. Advanced attacks will also try to manipulate their targets into performing an action that enables them to exploit the structural weaknesses of an organization. Unlike phishing emails, pretexting relies on building a false sense of trust with the victim, requiring the attacker to build a believable situation that leaves little room for doubt.

Baiting: Baiting is very similar to a phishing attack. What differentiates it from other types of social engineering is the promise of an item or information – fictitious things the hackers use to entice the victim. Baiting attacks are not restricted to online schemes, either. Attacks can also include the exploitation of human curiosity by utilizing physical media such as USB's.

best practices.

Stopping attacks like those listed above is simpler than you think – common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common red flags of a social engineering attack include the following:

- Someone creates a sense of urgency, trying to get you to respond quick and make a mistake.
- Someone asks for information they should not have access to or should already know.
- Someone asks for your password – no legitimate company will ever ask you for that.
- Someone pressures you to bypass or ignore security procedures or protocols.
- Someone promises something that is too good to be true (money or valuable goods).
- A friend or co-worker send you an email, but it appears suspicious or odd, not typical of that person. Reach out to that person through another means to confirm whether the email was in fact valid or malicious before replying or interacting with it at all.

data security.

Help protect yourself and your data against cyber crimes by implementing the following tips.

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?
Multi-factor 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. Multi-factor 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: cloud storage, external hard-drive, or a disk.

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.