Your Guide to Staying Safe Online

SUNBELT
Federal Credit Union

In Today's World It Is Harder Than Ever To Ensure Business and Personal Security Online...We've Got Tips You Need To Stay Secure...Learn More Inside!

Technology. It's a good thing, right? Think of all the things we can do on our computers that we couldn't do twenty years ago.

But as with most things in life, you have to take the good with the bad. And there is a lot of bad out in the cyber-world. The positive news is there are steps that you can take to protect yourself when you are online.

As the cybersecurity industry experts behind ThreatAdvice, we have prepared this guide to educate you on how to protect yourself online.

As Frank Abagnale, the "father of social engineering" said,"It's very important to always look at prevention. What can I do to make sure I'm not a victim? It's just like your house. How do I make sure I don't have a fire? Do I have smoke detectors? Do I have a fire extinguisher handy, that I don't keep things in my garage? What can I do to make sure I never have this problem?"

The key to prevention is education! This guide contains tips for using technology when you travel, how to prevent identity theft, what apps you should look for on your kid's iPhone and much more.

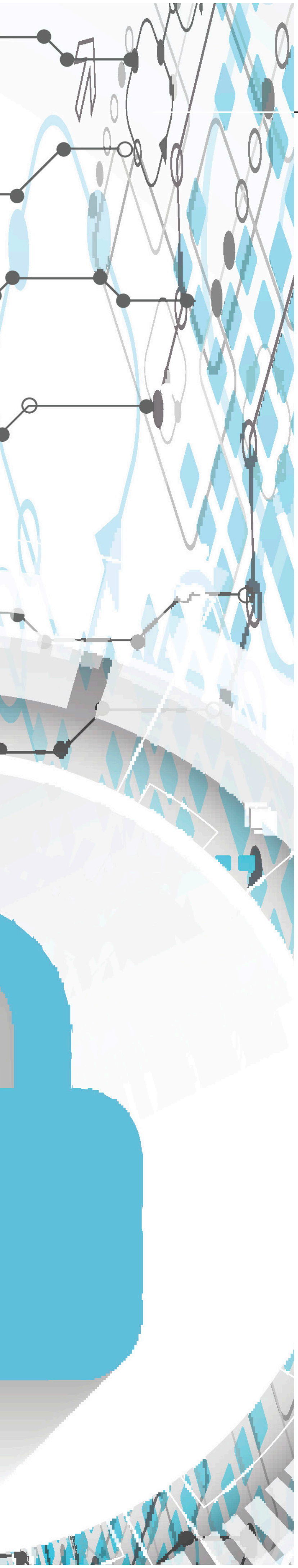


TABLE OF CONTENTS

SUNBELT Federal Credit Union

This online saftey guide is provided by ThreatAdvice. Please email info@threatadvice.com for information about reprints or with any questions or comments. For more information, visit www.threatadvice.com.

HOW TO PREVENT IDENTITY THEFT

We all know that identity theft is a big problem, and it can cause major headaches if you fall victim to it. However, there are some very effective steps you can take personally to help lessen the chances of becoming an Identity theft victim. Here are some of those steps:

1. Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary. Don't feel bad about refusing to give it out.

2. Don't respond to unsolicited requests for personal information (your name, birth date, Social Security number, or bank account number) by phone, mail, or online.

3. Review your credit report once a year to be certain that it doesn't include accounts that you have not opened. You can order it for free from Annualcreditreport.com. You can also contact the three credit reporting agencies to request a freeze of your credit reports.

4. Pay attention to your billing cycles. If bills or financial statements are late, contact the sender. Review your credit card and bank account statements. Promptly compare receipts with account statements. Watch for unauthorized transactions. Also, collect mail promptly. Place a hold on your mail when you are away from home for several days.

5. Enable the security features on mobile devices, especially if you have contacts, banking websites and applications saved. Also, don't ever use a public wi-fi network.

6. Shred receipts, credit offers, account statements, and expired credit cards to prevent "dumpster divers" from getting your personal information.

7. Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases.

“Just by taking some simple measures, you can greatly reduce the chances of having your identity stolen and having to deal with the pain that comes with it.”

8 APPS PARENTS SHOULD HAVE ON THE RADAR

Technology can be good as it allows us to keep in touch with our kids and teenagers, but it can also expose them to a variety of threats.

As a wise man once wrote, "There is nothing new under the sun." Of course, this adage still applies 3,000 years later to kids trying to fool parents about all manners of things, particularly their online activities. Not every pre-teen or teenager's online activity is bad or sinister of course, but technology has made it easier for kids to hide the sites they visit and things they do online from their parents.

Here are just a few of the apps to watch out for that can be used for less than noble reasons:

1 **Snapchat** - As you probably know, this is an app that allows you to send a photo or video from your phone and determine how long the person on the other end can see the image until it vanishes. Users think their snaps will disappear, but it's actually easy to recover a Snap, take a screenshot of it, and share it. Many snaps that were supposedly deleted have shown up online on revenge porn websites.

2 **Calculator%** - This app looks like an innocent calculator, but is actually used to hide photos. The use of this app was involved in a headline-making huge sexting ring case in Colorado. It uses a four-digit code to unlock a photo vault disguised beneath the "calculator."

3 **Vaulty** - Vaulty will not only store and hide photos and videos...it also snaps a photo of anyone who tries to access the "vault" with the wrong password. If this app is on your kid's phone, there is a high probability they are hiding something.

4 **Tinder** - Tinder is a popular app used for "dating" (and we use that word somewhat loosely) that allows users to match with other Tinder users in the surrounding area. The use of GPS makes it much too easy for your kid to be located by others, including unsavory adults.

5 **Audio Manager** - Audio Manager sounds innocuous enough in that it supposedly manages music audio for the user. However, it has nothing to do with that, and has everything to do with hiding photos, apps, and the like. This app is a favorite of kids who want to hide apps from their parents.

6 **Burn Note** - Burn Note is a messaging app that erases messages after a set period of time. Unlike Snapchat, this app is for text messages only. Interestingly, only one word is displayed at a time, creating a sense of secrecy to the messages. Because of promising true message deletion, kids tend to feel comfortable revealing more than what they would normally. However, it's possible to capture a screenshot so that the message can be shared, just like with Snapchat.

7 **KiK Messenger** - KiK is an instant messaging app that lets users exchange videos, photos, sketches and create gifs. And, unsurprisingly, the term "sext buddy" has been replaced with "KiK buddy." People have used Reddit and other forums to place classified ads for sex by giving out their KiK user names. This app has no parental controls, no user authentication and makes it easy for sexual predators to interact with minors.

8 **TikTok** - TikTok is a free social media app that lets you watch, create, and share videos—often to a soundtrack of the top hits in music. Because of this emphasis on popular music, many TIkToks contain swearing and sexually explicit lyrics. Video creators may perform suggestive dances and wear revealing clothing. If your child indicates he or she is 16 and the TikTok account is public, strangers can send private messages. TikTok now has a Family Pairing control where parents can link their child's account to their own to control direct messages, set screen time limits, and turn on/off restricted content directly from their phone. Be sure to explore that if your child has TikTok.

BY ALL MEANS TRAVEL, BUT MAKE SURE YOU ARE SAFE!

When preparing to embark on travel, certain steps seem natural: booking a hotel, reserving transport, and packing luggage. However, no matter if the intended travel is business or personal in nature, it is critical to undertake steps to ensure your safety on the road throughout your trip.

Understanding travel safety means understanding relevant risks and strategically planning to mitigate them. The reality is that both accidental loss and theft can occur while traveling; therefore in order to keep company data and your personal data protected, certain measures should be taken at each step of the voyage: before departure, during travel, and at the conclusion of the trip.

Another pre-trip aspect to consider is the preparation of your mobile devices.

Take the time to backup and update the devices that you anticipate taking with you. If you have items that are no longer needed, use this opportunity to delete them. Similarly if you are carrying data that you would not wish to share with the world, add an extra layer of protection through the encryption and password protection of the files.

It is also important to consider what travel information you are sharing, and with whom you are sharing it. Care should be taken with social media postings. Caution dictates that it is less dangerous to share those details and pictures after your return. You may also consider turning global positioning off on your pictures, so when posted to social media they do not geo-tag your exact location. Also, automated out-of-office messages should be concise and to the point. Distinguish between the messages that you are sharing internally and those that go out externally. Adding signatures or additional contact information to those external facing messages can increase the risk of that information being used by social engineers to potentially spear phish you or your colleagues.

Once embarking on your trip, stay close to your devices and baggage. Any item that holds your data should be taken with you onto a flight. If you're traveling by car, it is still important to keep important items in close proximity. Leaving items unattended or in a car is never a good idea. If you must go out without a device, make sure it has been secured in your absence. Hotel safes are a great place to keep devices, emergency payment cards, and important documents, including travel itineraries, a photocopy of your passport, etc.

In transit, in the airport, or anytime Wi-Fi and Bluetooth aren't in use, turn the features off on your devices. This will prevent the risk of unauthorized access, eavesdropping, or the

injection of a virus onto the device. When on the road, minimize your use of unknown WiFi signals. Public Wi-Fi can increase all kinds of risks, so use caution and best practices. Reserve sensitive corporate or financial tasks until utilizing a known, secure Internet source.

Remember too, in the event that an incident occurs while traveling, it is important to act quickly to minimize the potential harm. If for example a device is lost or stolen, quick reporting action to remotely wipe the device and change account passwords can mean stopping the loss of data.

Once home, monitoring and continued vigilance are advisable on all of your accounts. This would include financial accounts to check for suspicious charges, and even personal accounts like email. Taking certain proactive steps, like changing your passwords on relevant accounts and initiating an anti-virus scan on your devices, could help protect you and your data in the long run.

Travel has interminable benefits. It can provide opportunities for international team members to meet, or can generate a critical turning point for a project, or in the case of leisure travel, can reinvigorate the human spirit and reconnect families. The risks that we face in Information Security are not isolated to travel. We must be attentive to the protection of our data, both corporate and personal, at all times. However, by following these protective measures while traveling, we can work to ensure a more secure, productive, and enjoyable trip with a safe return.

Quick Travel Tips

1. Pack Sensibly

The principle of traveling light extends to data security. Travel with only the technology, devices and payment cards that you intend to use. Backup and update your devices, deleting any data or apps that are no longer needed. Also, carry photocopies of your important documents in case the actual documents are lost or stolen.

2. Transit Tenaciously

Be mindful of your personal items, devices, and luggage, especially at airport checkpoints. Take care to leave nothing behind. Carry-on devices and sensitive materials, and never leave items unattended.

3. Surf Securely

Open and unsecured Wi-Fi signals can pose a threat to data. Individuals broadcasting those signals can simultaneously be recording every keystroke as you type it. Choose instead to conduct your affairs on known, secure networks.

4. Be on Guard

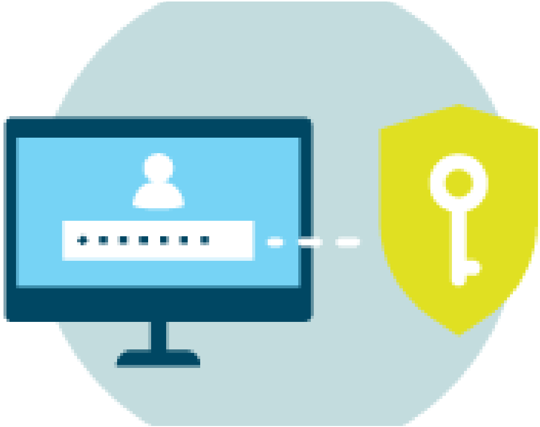
That old saying about keeping your wits about you is never truer than when traveling. Be aware of your surroundings, and monitor your email for travel warnings and travel alerts that may be issued during your trip. Report any suspicious activity or concerns to the appropriate contacts.

5. Have a Heedful Homecoming

Upon your return, continue to monitor your corporate, personal, and financial accounts for suspicious activity. Change your passwords as a proactive precaution, and scan your devices for signs of malicious software.

FRANK ABAGNALE'S ONLINE SAFETY TIPS

Frank Abagnale has been dubbed "the father of social engineering." His life story was captured in the hit movie "Catch Me If You Can" where Abagnale was played by Leonardo Dicaprio. Since then Abagnale has devoted 40+years of his life to assisting the FBI in fighting cyber crime. From his experience, here are some of his top tips to stay safe in today's cyber world!



Create Strong Passwords

We're required to generate passwords for different applications constantly, and it's important to remember a few basic rules. One good rule is: "a long password is a strong password." A 12 character minimum is a good rule of thumb. Also, use a mixture of numbers, letters (both upper and lower case), and symbols. Don't share your passwords with anyone, and don't write them down in plain sight. Don't use easy to recognize themes such as your last name or birthday, and use different passwords for every application. Change your passwords often, and use a good password manager to store them. Remember: your passwords are the gateway into many important parts of your life, so to ensure safety, you must use good password hygiene consistently.

Mobile Device Security

Most people don't realize that their phones, tablets, and other mobile devices are a huge target for hackers. Instinctively we think our mobile devices don't have the same security concerns as our desktop work computers, but that's far from the truth. Hackers love to target these devices, and, as users, we must employ the same security practices, such as data encryption, strong passwords, updating all security patches, and dual authentication. Treat your mobile devices like super computers - because that's basically what they are.

Security Perils of Social Media

Obviously social media is a huge part of everyday life, and that's not going to change anytime soon. The bad guys know this and have figured out some clever ways to take advantage of it. Someone can assume the identity of a corporate customer or an executive and manipulate corporate social media platforms, or even plant malicious links at popular places to visit on social media. Many times, scams centered around surveys or winning prizes are used. When you see a story that Brad Pitt has been killed in a terrible helicopter accident, think before clicking on the link. The moral of the story is be ever cautious when using social media platforms, because things are not always what they seem.

Beware of Vishing

Vishing, or voice phishing, is a form of criminal phone fraud that uses social engineering over the phone to gain access to private personal and financial information. Vishing frequently involves a criminal pretending, over the phone, to represent a trusted institution, company, or government agency. You may be asked to buy an extended warranty, offered a vacation, told your computer is infected and you need anti-virus software, or asked to donate to charity. Basically, vishing is a new name for the age-old telephone scam. To conduct these scams, vishers often use modern voice over IP features such as caller ID spoofing and automated systems that make it difficult for authorities to monitor, trace or block their activities. They'll stop at nothing to achieve their goals - and use of the good old-fashioned phone is still in vogue. With phones more than ever being a constant part of our lives, it's very important to be skeptical and diligent at all times.

Fake News: What Is It And How Not To Fall Victim To It

Half of all adults in the United States consider fake news a major problem. Read these tips to know how to make sure what you are reading is actually true!

Delete "Facebook"?

Deleting this app will also delete its data.

One of the newest and most interesting social engineering scams of late is something you've surely heard about recently - fake news stories. While the internet is a great thing, it also is a blank canvas for anyone to put out any information they desire, regardless of whether it's accurate or not.

Fake news can be put out for several reasons such as:

- Trying to influence opinions
- Manipulating financial markets
- Direct attacks on business competitors or other opponents
- Selling advertising
- Trying to trick folks into clicking on malicious links

These fake news stories (and fake advertisings) are some of the most difficult to spot social engineering scams.

Where does fake news originate? These stories can come through;

Tweets
Facebook posts
Digital images
Journalistic sites that publish content without fact checking.
There also are many sites pretending to be real news organizations but they only publish fake news stories. Oh, for the good ole days of Walter Cronkite!

How do fake news stories affect business enterprises?

Stock prices can be dramatically altered with fake news stories about the company. Just think about false information being spread about earnings, executive appointments, firings, or mergers and acquisitions. These can have devastating and lasting effects on a business. Also, a company can lose a substantial amount of goodwill with its customers and markets if fake news stories circulate.

Even if these fake stories are immediately proven to be false, the damage is already done since "everything on the internet is true"-NOT!

What can you do to ensure you don't fall victim to fake news?

- Avoid websites that end in "lo" such as Newslo. These more than likely are fake news platforms.
- Avoid websites that end in ".com.co" or the like. Unusual domain names are a huge red flag.
- If reputable news sources are not reporting on the story, then it's most likely fake.
- Use sites such as Snopes to verify the accuracy.
- Watch out for bad grammar-this always warrants great caution.

The bad guys will try everything to make life miserable for the good guys, and fake news stories are just another example. Most of the time, if it's too good, too sensational or too devastating to be true, then it probably isn't real!

Protect yourself from potentially dangerous text messages.

STAY ALERT.

EVERYTHING YOU NEED TO KNOW ABOUT SMISHING!

What is “Smishing?

SMS phishing, known as “smishing,” is a phishing attack through SMS messaging. These attacks look like text messages from reputable companies that ask their targets for personal information or to click a malicious link.

98% of SMS messages are read within one second of being received.

This statistic makes SMS phishing very attractive to scammers and hackers. SMS phishing has been on the rise due to the rapidity of text messages and the simple fact that most people own smart phones with the capability to fill out information and click links. Many businesses and institutions have started sending confirmation links and messages through SMS. Cyber criminals have taken advantage of this and turned it into an easier way to breach personal information and businesses’ confidential data.

Defend Against Smishing

The importance of education and prevention against SMS phishing attacks and breaches is just as important as any other cybersecurity measure. Smishing attacks can be even less suspicious than email attacks and other cyber breaches because text messages are so frequent and people are very quick to open and click. Hackers will use their advantage and try to impersonate your financial institution, shipping service and a wide variety of other entities to send messages that look legitimate to you.

Cybersecurity practices against SMS phishing lines up with practices you take against email phishing scams. It is important to remember never to give out personal or financial information to unsolicited or unknown sources, over the phone or via text. This cannot only put yourself at risk, but also your business or workplace if you have confidential business information on your cell phone.

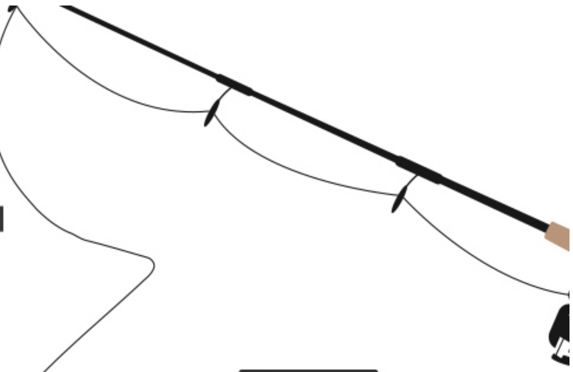
What should you do when you receive an SMS Phishing Scam?

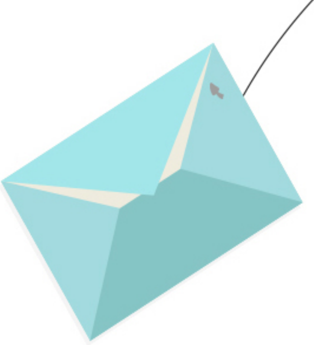
Some tips when it comes to protecting against SMS phishing line up nearly one to one with protecting against email phishing attacks. Traditional cyber security training for phishing attacks can translate over to training for SMS phishing attacks.

- Never give out personal information.
- Do not click unsolicited links.
- Read the message closely. Check for spelling errors and grammar mistakes.
- Check for verbiage such as “act fast” or sign up now or any language that is pushy, encouraging a quick action.
- Look into the sender’s telephone number. Verify that the phone number matches the company’s phone number. If you have received legitimate SMS messages from that company or institution before, check to see if the phone number matches previous messages you have received.
- When in doubt, give a call to the institution to inquire.

> *“Unfortunately, threat actors are continuing to look for new ways to compromise businesses and individuals. As soon as we start to get a handle on one method, they have another new method that they utilize. The only way we can fight the bad guys is through continual education, awareness and simulation exercises.”* - **Will Blackburn, CTO, ThreatAdvice**

DON'T TAKE THE BAIT





WHAT IS PHISHING?

Phishing is a form of **cybercrime**, whereby an individual attempts to deceive an email recipient with a fraudulent correspondence, often attempting to steal identity credentials, proprietary data, or as a means to deliver malicious software.

KNOW WHAT TO LOOK FOR

Learning to **identify** the telltale signs of a phishing email is important for your security. Check the full email address of the sender for legitimacy. Review the content of the message for strange tone or writing/grammar mistakes. Finally always be wary of hyperlinks and unsolicited attachments.

BE VIGILANT

Phishing can happen any time. Always take the time to **review** your emails, be aware of the risks, delete and report suspicious activity, and maintain your software and systems keeping them up to date.

BE DILIGENT

While you cannot prevent criminals from attempting an attack, there are some simple steps you can take to thwart their success.

- **Consider** if the message makes sense
- **Confirm** the link by hovering over
- **Ask** the sender directly instead of replying to the suspicious email
- **Open** attachments with care
- **Keep** your computer updated
- **Keep** your Anti-Virus software updated