Data Security Presentation

Informational Packet

Presented by:
Randy Hunt, State Representative 5th Barnstable
Room 136, State House
Boston, MA 02133
(617) 722-2800 x8743

Table of Contents

1. Introduction

Cape Cod is a unique area in Massachusetts and, for that matter, anywhere. As much as we appreciate the throwback to earlier times, the mom-and-pop stores, the clam shacks, kids playing on the beach, we are just as much part of the 21st century as anyone else in this state or country.

The ever growing presence of the internet in our daily lives can prove very beneficial, allowing for a vast expanse of knowledge at your fingertips and the ability to connect with anyone all over the world. However, lurking under cover of unbelievable news stories you have to see to believe, promises of offers too good to be true, and seemingly innocent online interactions, are hackers and scammers desperate to get a hold of important private information. According to recent studies, there is a hacker attack every 39 seconds, affecting 1 in 3 Americans every year.

Data hackers do not only target individuals but will also attack major companies that people have trusted with private and personal information. From May to July of 2017, Equifax was the subject of a data hack that stole the personal information of over 148 million Americans, upwards of 75% of our adult population that relies of credit transactions. House Bill 4806, An Act Relative to Consumer Protection from Security Breaches, which passed the House and Senate unanimously on July 25, eliminates charges to freeze your credit account with Equifax and other credit reporting agencies, and hold companies accountable for failing to protect consumers.

Representative Randy Hunt served on the conference committee for this bill to ensure the most optimal outcome to benefit consumers and victims of this personal data breach. In addition to the work on the consumer credit bill, Representative Hunt feels it is equally as important to stress safe practices on the internet in order for individuals to protect themselves. This presentation will discuss how you can to protect yourself from a data breach, techniques to use every day when on the internet, and how to avoid falling victim to common email and phone scams.

If you have any further questions, please feel free to contact Randy through his legislative office. His aide, Katie Babbin, can be reached at katelyn.babbin@mahouse.gov or (617) 722-2800 x8743.

2. Equifax Breach

House Bill 4806, passed this year, requires credit companies subject to data breach to pay for at least 5 years of credit monitoring with no cost to the consumer, and would prevent credit reporting agencies from extracting waivers from consumers in these situations, thus preserving our rights to take legal action when companies prove to be unreliable keepers of our personal information.

If you fear that you may have been a victim of the Equifax breach there are steps you can take to check and add additional protections. By visiting www.EquifaxSecurity2017.com you are able to view new consumer updates that are posted and check the potential impact the Equifax breach may have had on you. To do so, click the box, "Am I Impacted?" (IMPORTANT: check to make sure you are on a secure webpage and using private Wi-Fi; for information on this see page 10). Once on this page, enter your last name and last six digits of your social security number > click on the box "I am not a robot" > click continue. You will receive a message either indicating the Equifax believes "your personal information may have been impacted by this incident" or "your personal information was not impacted by this incident."

If you were impacted in this data breach, you can choose to enroll in Equifax' TrustedID Premier Program. This Program offers credit file monitoring with the purpose of alerting customers of any attempts to access their information or open credit/loan accounts without their permission. According to Equifax, consumers who sign up for TrustedID Premier will not be automatically enrolled or charged after the conclusion of the complementary year of TrustedID Premier. Since the passing of H4806, Equifax has extended the one-year credit monitoring at no charge.

There are three major credit reporting bureaus: Equifax, Experian, and TransUnion. If you plan to file a fraud alert or freeze your credit file, make sure you do this with all three credit reporting bureaus.

To freeze your credit file:

Equifax:
💻: https://www.equifax.com/personal/credit-report-services/
☎: (800) 525-6285

Experian:
💻: https://www.experian.com/freeze/center.html
☎: 1 (888) 397-3742

TransUnion:
💻: https://www.transunion.com/credit-freeze
☎: (888) 909-8872

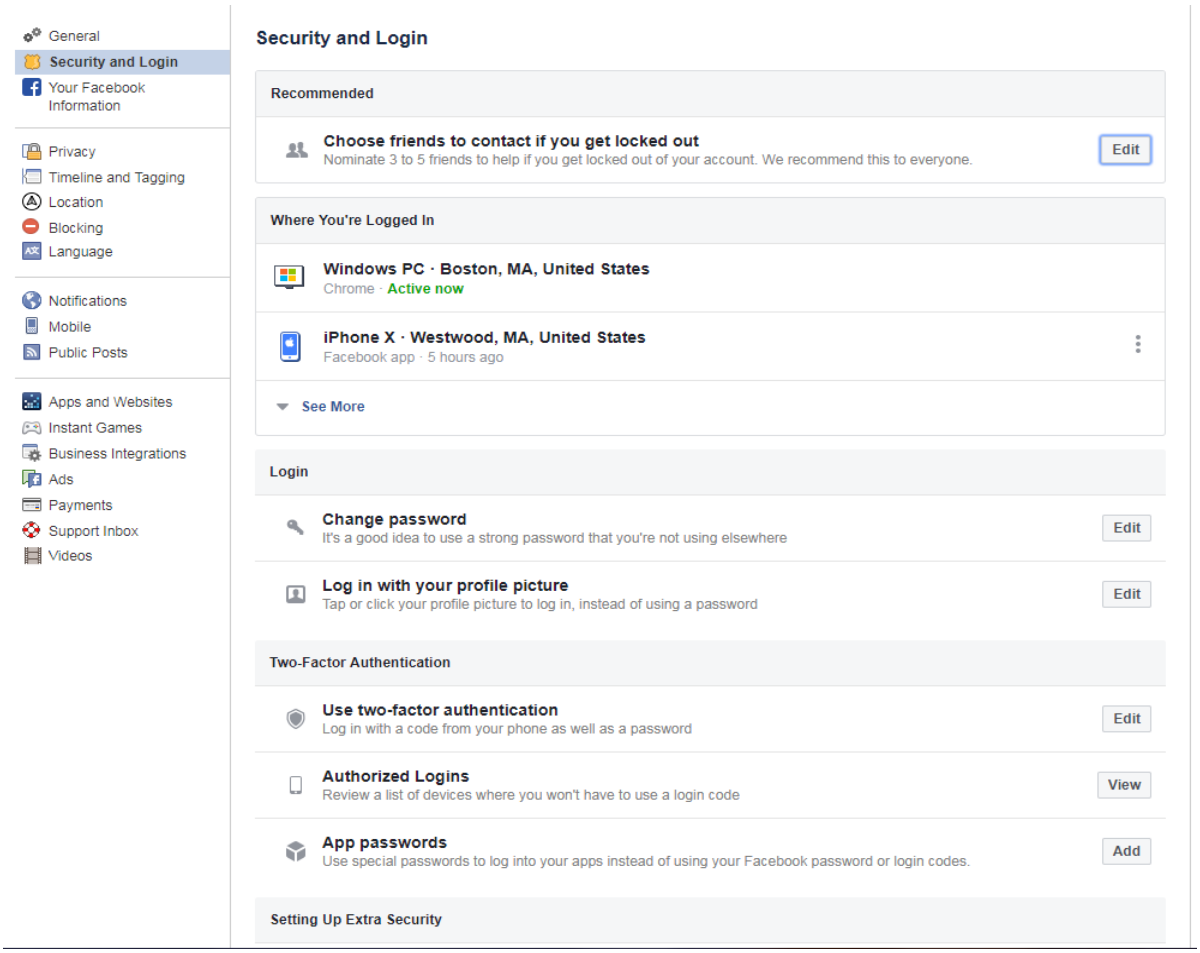
3. Safe Usage of the Internet

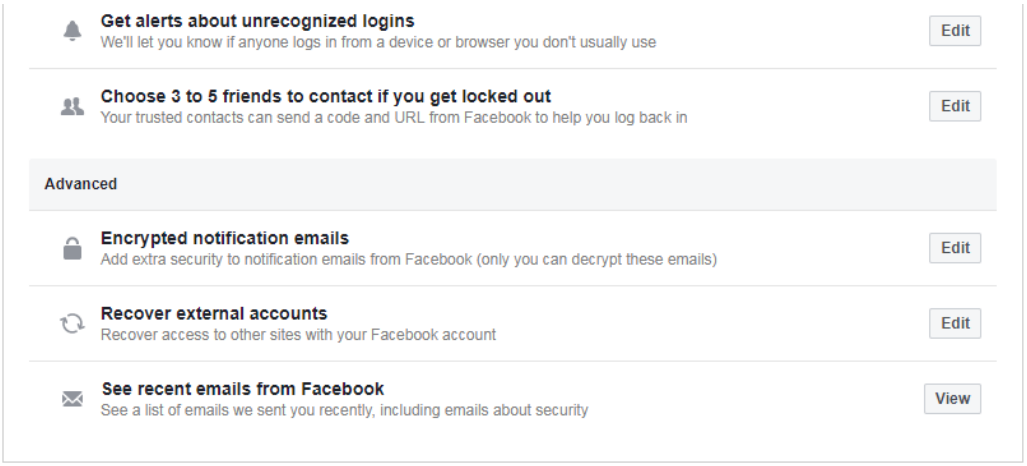
On many websites that require you to have an account, there are a range of privacy settings that you can adjust to protect yourself online.

Facebook

To access your Facebook account settings locate the blue tool bar across the top of the webpage > select the drop down arrow on the right side of the bar > click settings

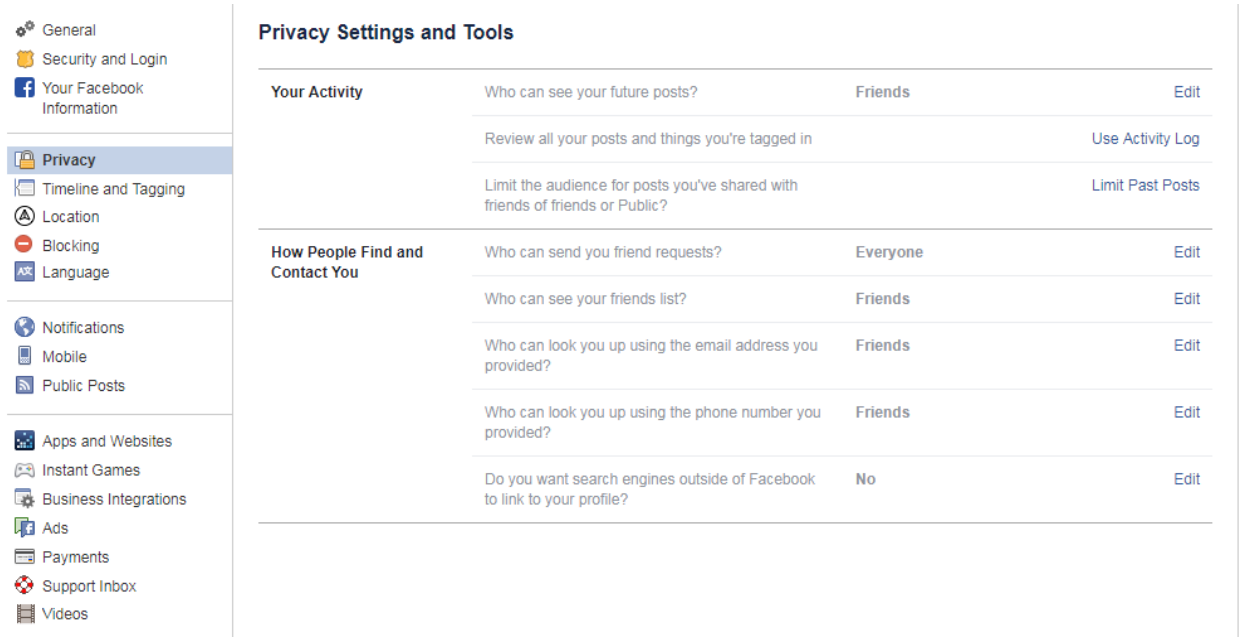
Security and Login





From this page you can view recent login attempts and report any you do not recognize, change the password to your account, set up two-factor authorization of login attempts to your account which would require an access code sent to your phone or email to log into your account along with your password, set up alert notifications for login attempts, and see a list of recent emails sent to you from Facebook, allowing you to differentiate between a legitimate email from Facebook or a scam email claiming to be from Facebook.

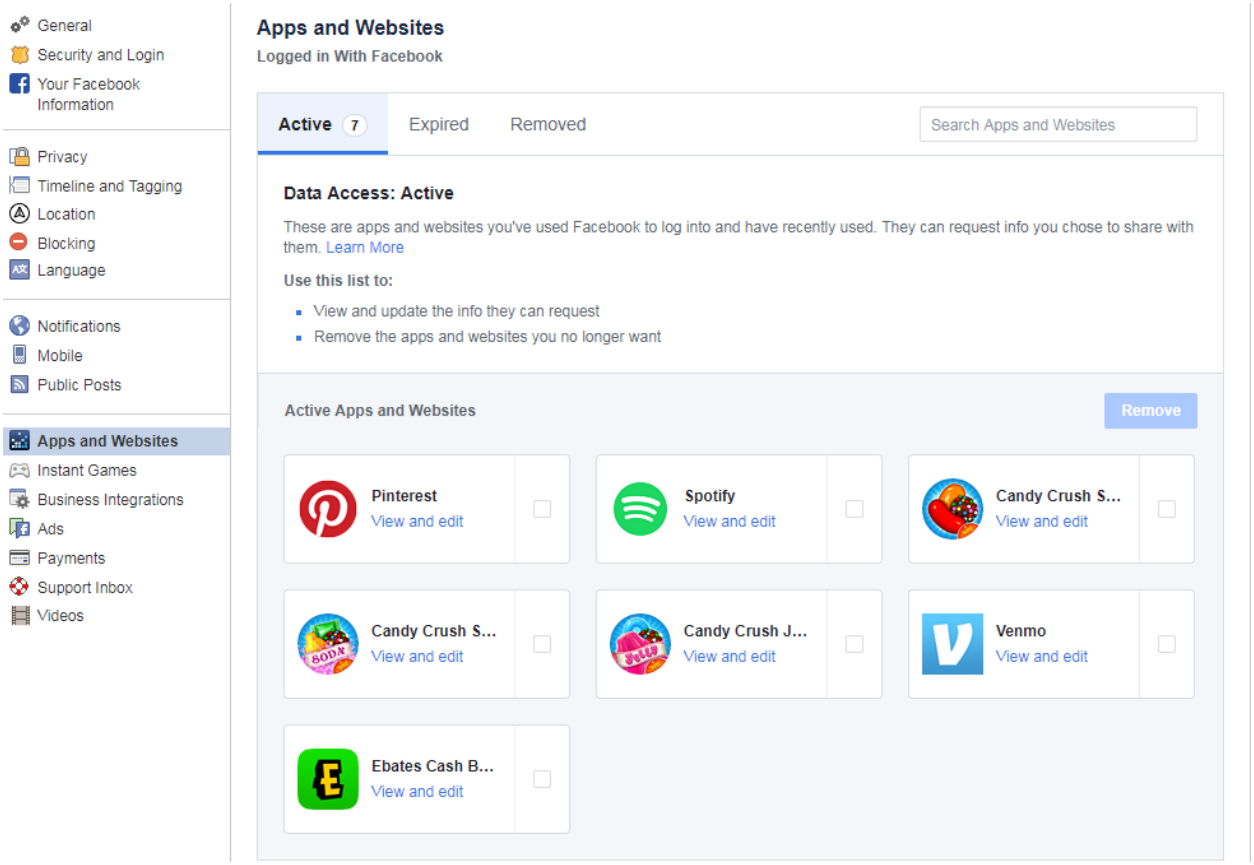
Privacy



Your Activity: choose your audience for your future posts, review your activity log, and limit the audience of your past posts.

How People Find and Contact you: control who can send you friend requests, who can see who you are friends with, who can look you up using the email you provided to make your Facebook account, who can look you up using the phone number you provided, and the ability for search engines outside of Facebook to link to your Facebook account.

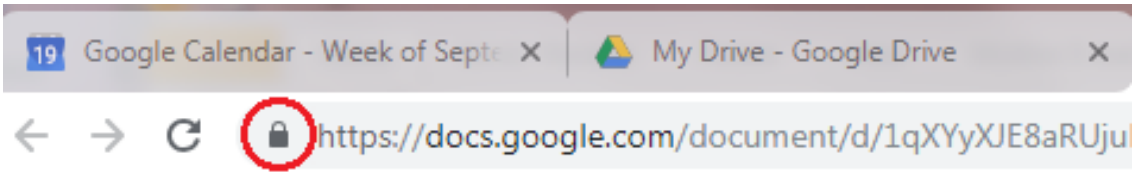
Apps and Websites



On this page you can choose which apps and websites have access to your data. To remove access> click on the box next to the app you want to remove> click remove. IMPORTANT: You will no longer be able to sign into those apps and websites using your Facebook login, make sure you create new login credentials for them before you remove access.

Safe Browsing Tips and Tricks

1. A secure website is identified either through “https”, s= secure or most internet browsers will display a lock icon and state that the site you are on is secure in the URL bar.



2. Avoid Clickbait. Clickbait is links to articles or webpages with headlines specifically designed to entice you to click on it. Usually leads to unsecure sites trying to sell you something and access your personal information.

3. Avoid making online transactions or accessing personal information when using public Wi-Fi.

4. Only download from trusted sites. Suspicious downloads could lead to Malware in disguise.

5. Use discretion during online interactions. Common scams are receiving a friend request from someone you know and are already friends with and receiving Facebook messages claiming to be a friend asking for personal information. Always try to confirm the identity of the person before accepting or disclosing personal information.

6. Get Antivirus software and make sure it is up to date.

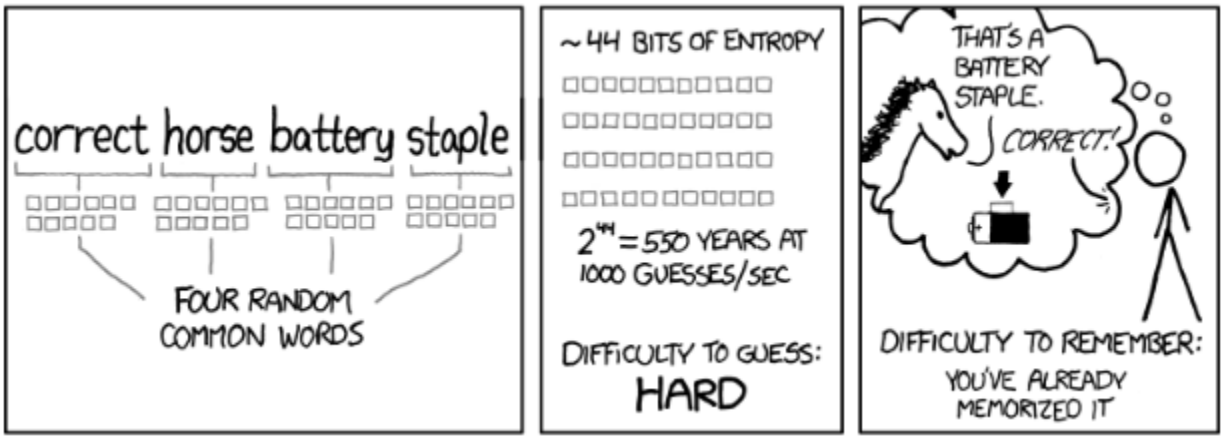
4. Password Strategies

The longer the password is the harder it is to crack and unfortunately the harder it is to remember it. It is also very important to use a different password for everything. Here are some techniques to help you develop a secure password that is easy to remember.

<u>Take a sentence and turn it into a password:</u>
Examples:

- WOO!TPwontSB= Woohoo! The Patriots won the Super Bowl.
- PPupmoarT@O@tgs= Please pick up more Toasty O's at the grocery store.
- 1tubuupshhh...imj= I tuck button up shirts into my jeans.
- W?ow?imp::ohth3r = Where oh where is my pear? Oh, there.

<u>Use a Passphrase:</u>



If you are still having difficulty remembering longer passwords, password management tools like Lastpass, 1password, and Dashlane can be downloaded to your browser or mobile device to store all of your passwords.

5. Email Scams

According to a Symantec study, by the end of 2017, the average user was receiving 16 malicious emails a month. The frequency of email based scams is increasing. Below are common examples of email scams, how to recognize them, and strategies you can use to protect yourself.

Phishing

Phishing emails are one of the most common and difficult to identify email scam. They are convincing emails stating that there has been a security breach to an account and you need to sign in immediately to confirm your identity and secure your account. These emails often contain links to fake websites that look very real. These emails are designed to lure you into giving login credentials, alternate forms of payment and other personal information, i.e. SSNs.

Nigerian Prince

One of the oldest forms of email scams. The emailer claims to be in a position of wealth and power, offering you a large sum of money for small tasks. Rule of thumb: if it's too good to be true it probably is. Do not respond to these emails or divulge private information.

Lottery Scams

Exciting claims that you won the lottery but first require that you pay a "processing fee." They will ask you for payment information in order to charge you for that fee, giving them access to your money and identity.

Advanced fees for guaranteed loan or credit card

These emails claim that you qualify for a pre-approved loan or credit card as long as you pay up front fees. No legitimate loan or credit card company will ever ask you to pay up front fees for pre-approved qualifications.

Offer to pay more than asking price on goods for sale

This is a common email scam in response to an ad you placed on a public site like Craigslist. The offer will be for much higher than the asking price to account for extra fees i.e., “international fees.” Payment will usually be sent to you by money order or cashier's checks that are either not authorized or are forged.

Employment search scams

These emails offer a position as a “financial representative” to handle payments from US customers. In order to pay you, they claim they need access to your bank account information. Results of this scam include identity theft, emptied bank accounts, receiving fake money orders and checks, etc.

Charity scams

A very common response to a tragedy today is to set up charity websites to benefit the affected families. Unfortunately scammers have taken advantage of this by creating fake charity websites to steal donations. If the request comes by email it is most likely a phishing scam, do not click any links.

Travel Scams

Travel Scam emails offer amazingly low fares but require you to book immediately. These offers hide drastically overpriced fees that do not show up until after you sign. Often cannot get reimbursed if you choose to cancel.

“Make Money Fast” Chain Emails

Pyramid Scheme! These emails ask you to send money to people on a list and forward the email to a certain number of people. The promise is that your name will be added to the list and so in return you will have money sent to you during the next round. Often the list is fixed and the top names do not move so you will never be sent money. Pyramid Schemes are illegal; if you participate you can be charged with fraud.

6. Phone Scams and Robo Calls

It has been estimated that one in every 10 adults has been a victim of phone based scams, up nearly 60% from the previous year. Like email scams, these numbers are also on the rise. Most phone scammers are after your money and attempt to make you give them information by pressuring you to act fast or threatening you with claims that you owe money. It is important to recognize some tell-tale signs of a phone scam and to never disclose personal information without verifying the call.

Some common signs of a phone scam:

- "You've been specifically selected (for this offer)"
- "You've won one of five valuable prizes"
- "This investment is low risk and provides a higher return than anywhere else"
- "You have to make-up your mind right away"
- "You don't need to check our company with anyone"
- "We'll just put the shipping and handling charges on your credit card"

If you hear anything that sounds like this, hang up and report these calls to the FTC (see page 19).

Questions to ask Yourself:

<u>Who is calling...and why?</u>

Telemarketers must tell you it is a sales call, the name of the seller, and what they are selling before they make a pitch. If they do not give you this information, hang up.

What's the hurry?

It is very common for a scammer to talk very fast and claim you are on a tight timeline. Most legitimate businesses will give you time and written information about an offer before asking you to commit to a purchase.

If what they are offering is free, why are they asking me to pay?

Scammers will offer you prizes or gifts but claim you need to give them payment information in order to cover fees or shipping and handling. If you have to pay, it's a purchase not a prize or a gift.

Why am I "confirming" my account information or giving it out?

Some callers already have your billing information before they call you. They are looking for a verbal confirmation from you so they can claim you approved a charge.

How to handle a pre-recorded call or Robocall:

Hang up the phone. Don't press 1 to speak to a live operator or any other key to take your number off the list. It will not work, and will often lead to more robocalls.

IRS Phone Scam

A very common and scary phone scam, involves scammers claiming to be from the IRS requesting immediate payment for overdue payments and threats of jail time if you do not apply. The IRS is aware of this scam and has listed on their website ways to recognize when you are being victimized.

The IRS will never ask for credit card, debit card, or prepaid card information over the phone, insist that taxpayers use a specific payment method to pay tax obligations, request immediate payment over the phone, and will not take enforcement action immediately following a phone conversation. Taxpayers always receive prior written notification of IRS enforcement action involving IRS tax liens or levies.

Calls from a local number or your own number

This technique is engaged by scammers because you are more likely to pick up the phone if you recognize the number. If you do not recognize the full number, or if you get a call from your own number, do NOT pick up. If a local number is legitimately trying to get in touch with you they will most likely leave a voicemail. Answering the phone when you see your own number is understandingly very tempting but it will not make the scammer less likely to use your number again. If you do not answer they will eventually mark your number as ineffective and move on.

The “Can you hear me now?” scam

This scam is quick and dangerous. A lot of companies use voice authorization to confirm purchases over the phone. The goal of this scam is to get you to say “yes” so that they can record that and use it to authorize other purchases or access to come of your accounts. It is important that if you are asked yes or no questions to answer carefully until you can confirm if the call is legitimate.

Example:

Phone rings. You hear some clattering in the background, and then the operator comes on and says "I'm sorry, I dropped my headset. Can you hear me okay?" You say "Yes" and they've got it on their recording to be used to cut a tape that goes like this:

Operator: “Do you accept the terms of our offer and that you'll be charged $20 per month through your Verizon bill?”

You: “Yes”.

All they need is the recording of you saying "Yes" and they're good to go. You don't even have to stay on the line long enough to hear about their scam.

7. Resources

Free Credit File Report

💻: www.annualcreditreport.com

☎: 877-322-8228

Report Robocalls to the FTC

💻: www.ftccomplaintassistant.gov

☎: 1-888-382-1222

National Do Not Call List

Register your home and mobile numbers, report continued calling

💻: www.donotcall.gov

Mobile Phone Carrier Robocall Blocking

Verizon

💻: https://www.verizon.com/about/news/there-are-options-for-blocking-robocalls

AT&T

💻: https://www.att.com/features/security-apps.html

T-Mobile

💻:https://www.t-mobile.com/news/scam-block

Sprint

💻:https://www.sprint.com/en/support/solutions/services/block-restrict-or-allow-voice-calls-using-my-sprint.html

Elder Hotline

Scam awareness and Telemarketing reporting

☎: 1-888-AG-ELDER (1-888-243-5337)

IRS Identity Protection Information

💻: https://www.irs.gov/identity-theft-fraud-scams

Mass DOR Identity Theft Information

💻: https://www.mass.gov/info-details/protect-yourself-against-tax-identity-theft