Scam Alert!
What to Look For and How to Protect Yourself

A Presentation by Christopher Gallo, CPA

to the Rotary Club of Bridgeport

January 21, 2020

A Few Caveats

- I will be moving very quickly through this material…
- The presentation will be posted on our Club's website…
- There is something new everyday regarding scams!
- While I am not an expert…I can *help you* ***if*** you have an issue!

Some Basics

- Scams come in all sizes and shapes but have one thing in common…*tricking you* into parting with your hard-earned cash.
- Fraudsters can use deception or even *terror* and *fear tactics*.
- They may even *make you think* they are the police, the government, a lawyer or even someone you know.
- The message may get delivered via a threatening telephone call, email or an *official-looking* letter.
- But don’t worry…*if you know you haven’t done anything wrong…you should be ok*.

The Most Important Thing to Remember…

No government agency *will ever demand* that you pay by gift card, credit card, wiring money, or *bitcoin*.

Common Scams – IRS Imposter Scams

- A phone call from someone who says they are from the IRS and you *owe the IRS back taxes*. (They may even give you their IRS identification badge number.)
- You are threatened with a lawsuit, revoking your license, impending arrest or deportation.
- Caller ID shows call is from Washington DC (Area code 201).
- You are told to put “what you owe” onto a prepaid debit card then call back with the card number.
- They may even know your Social Security Number (SSN).

Common Scams – IRS Imposter Scams

Know this:

- The IRS *will never ask you to pay* with prepaid debit cards, wire transfers, or *Bitcoins*.
- If you do owe back taxes, you will get a letter, not a phone call.
- Caller IDs can be easily faked.
- The "**Bureau of Tax Enforcement**" does not exist!

Common Scams – "You've Won the Lottery"

- A phone call (or email) from someone who says…you've won the lottery (or a trip, sweepstakes, or some other valuable prize). *But first*, you need to pay the taxes on your winnings before you can get your money.
- You are told to put "what you owe" onto a prepaid debit card then call back with the card number.
- Or send cash/check to some "Agent" to "insure" delivery.

Common Scams – Fake Debt Collectors

- They want to steal your identity and ask for:
  1. Credit card numbers
  2. Checking or savings account numbers
  3. Social Security Numbers (SSN)
  4. Birthdates
  5. Driver's license number
- What they will do:
  - Write fraudulent checks on your account
  - Take out loans using your name, address and SSN
  - Run up bills in your name

Common Scams – Social Security Scam

- An urgent phone call (or email) from someone who says…your Social Security *benefits are in danger of ending* or your *SSN will be suspended* unless you… (do what I tell you to do.)
- Ask you to *confirm your SSN* or ask for other information, such as…your bank account to "*redirect*" your Social Security check.
- Social Security Administration will never threaten or extort you, end your benefits or suspend your SSN.
- Your best defense…just *Hang Up*!

Common Scams – Grandkids Scam

- You get an urgent call: “Grandma, I’m in trouble and I need some money for … bail, a medical bill or something else.”
- They tell you not to tell anyone.
- What should you do?
  1. Call the grandchild or someone else in the family
  2. Tell the caller you need to check this out… “How can I get back to you?”
- What you will not do…send any money!

Other Scams

- Health Care -> You don't need that new Medicare card.
  - They just want your SSN and your money.
  - Walk away!
- Home Repair -> A storm has damaged your home.
  - They pressure you to sign a contract *NOW* and need a down-payment today.
  - Call your insurance person and get other estimates.
  - Get references whenever you need home repairs.
- Charity Fraud -> Common after a natural disaster somewhere.
  - The charity sounds familiar but it's a scam.
  - Don't be afraid to say…"No thanks!"
  - Hang up!

Other Scams

- Spoof phone calls -> The phone number looks familiar.
  - If it's important, they will leave a message!
- "You pre-qualify for a low cost credit card or loan"
  - You pay the fee but the card or cash never arrives.
- Money-mule scam -> Someone sends you a check and asks you to forward a portion of the amount to a 3rd party.
  - *Don't do it*.
  - The check will initially clear but a week or two later, the bank will charge your account because the check was a phony!
  - You could be charged with *participating in a crime*!

Tech Support Scam

- Caller says they're from Microsoft or AppleCare.
- Caller says your computer has a virus or malware.
- They will ask for remote access to your computer.
- These scammers want to:
  1. Sell you useless software or services
  2. Steal your credit card number
  3. Install malware so they can access the data on your computer
- Hang up!
- Never give control of your computer to someone you don't know.

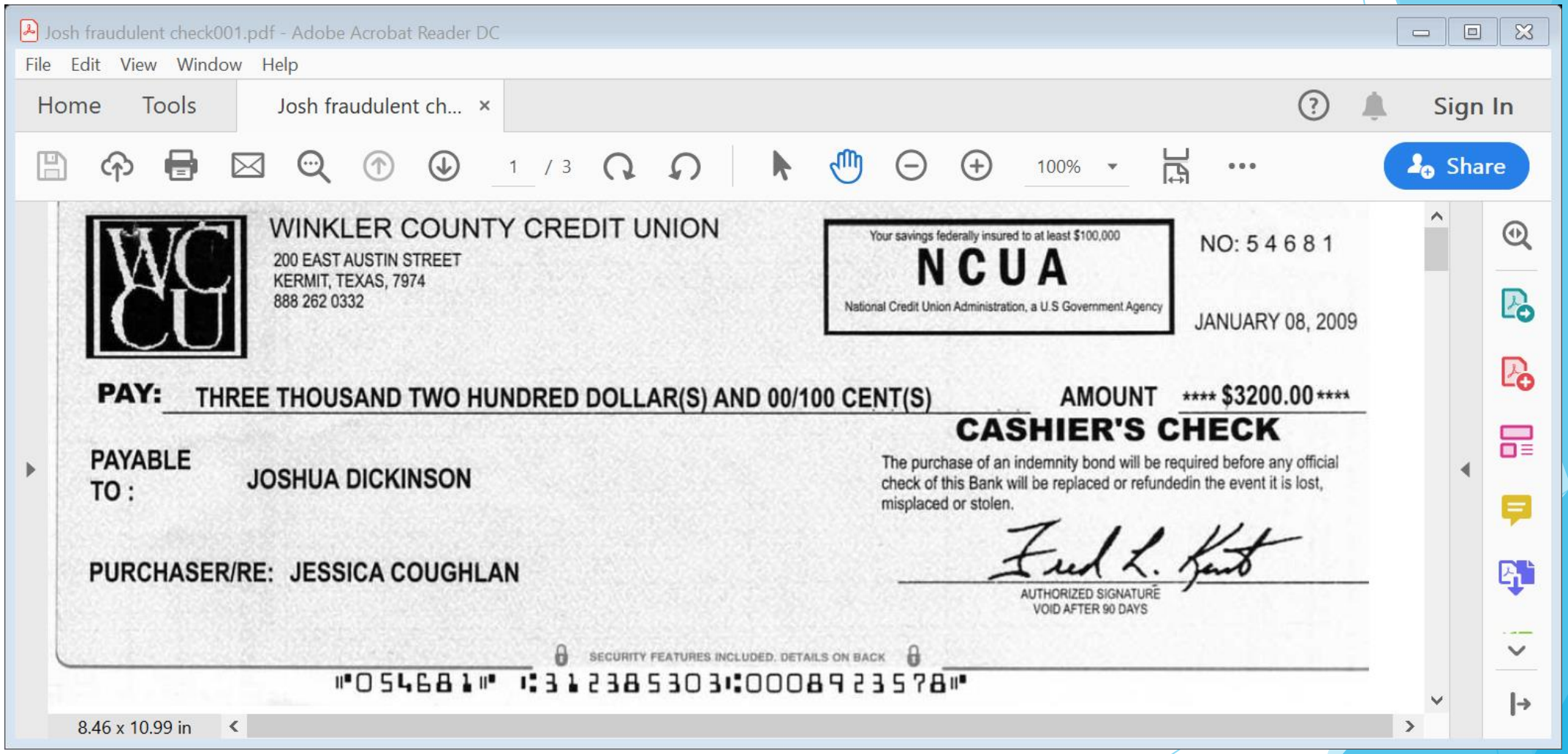
How to Beat "Robo-Call" Scams

1. ***Never answer calls from numbers you don't recognize***! *Don't engage with the caller!*
2. ***Hang up the phone*** once you sense the caller is a scammer.
3. ***Don't press any keys*** even if they say, "Press 1 to remove yourself from this call list."
4. ***Don't wire money or send a check/money order*** to anyone. Once you send it, there is no way to trace it. ***Lost$$***
5. ***Never deposit a "winnings" check*** and then wire money back or to someone else. The check will bounce, and you're stuck.
6. Put your phone numbers on the Do Not Call Registry… www.donotcall.gov or 888.382.1222.

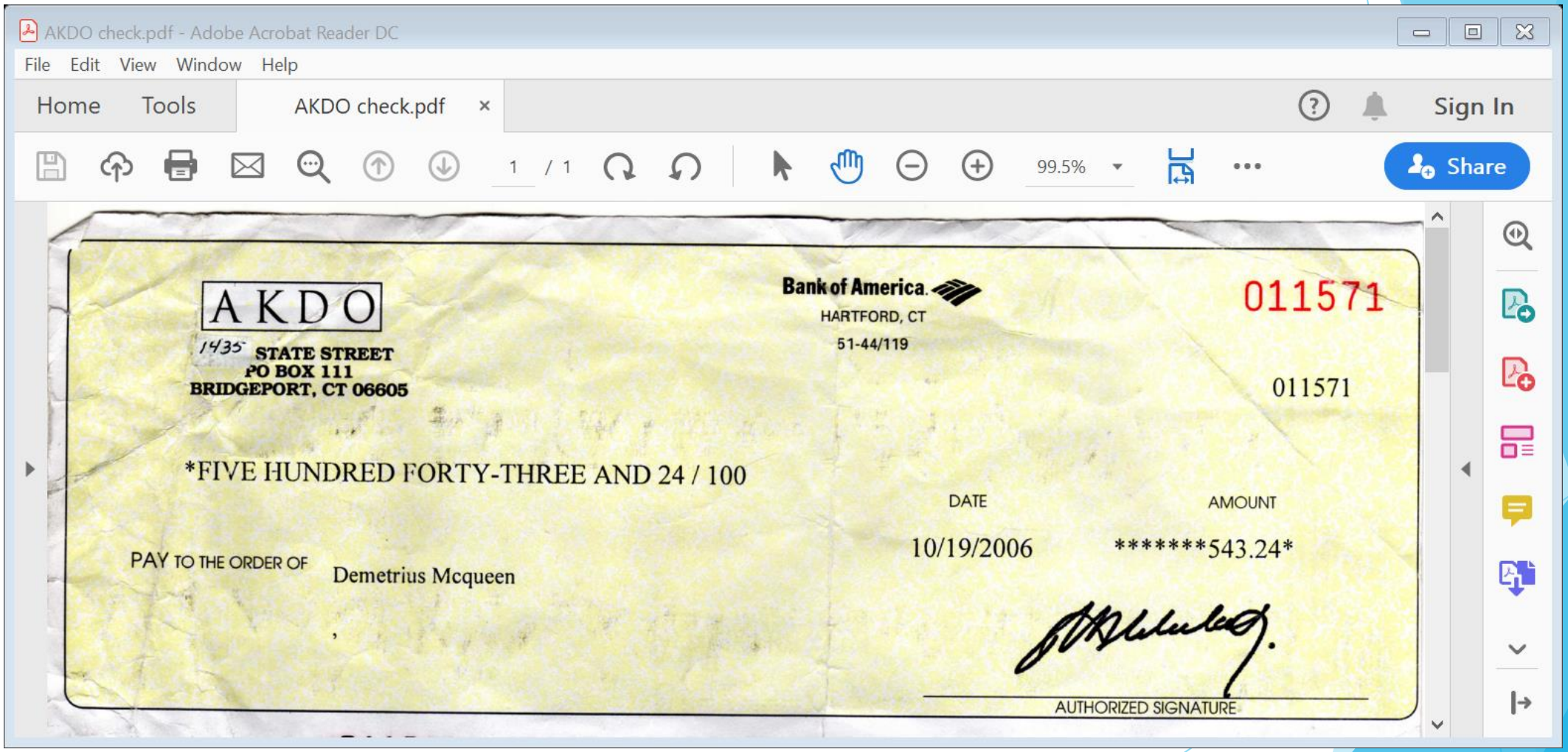
Other Tips to Beat Scams

1. Protect your sensitive financial information…bank account numbers, credit cards, SSN, birthdates, etc.
2. Review activity in your bank accounts *frequently*.
3. Look at *all* charges on your credit card statements.
4. Check your credit report.
5. Read your Medical Insurance "Explanation of Benefits"
6. Use strong passwords online.
7. Shred documents with sensitive personal information.

Real Frauds


Josh fraudulent check001.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools
Josh fraudulent ch...
Sign In
1 / 3
100%
Share
WINKLER COUNTY CREDIT UNION
200 EAST AUSTIN STREET
KERMIT, TEXAS, 7974
888 262 0332
Your savings federally insured to at least $100,000
NCUA
National Credit Union Administration, a U.S Government Agency
NO: 54681
JANUARY 08, 2009
PAY: THREE THOUSAND TWO HUNDRED DOLLAR(S) AND 00/100 CENT(S)
AMOUNT **** $3200.00 ****
CASHIER'S CHECK
PAYABLE TO : JOSHUA DICKINSON
The purchase of an indemnity bond will be required before any official check of this Bank will be replaced or refundedin the event it is lost, misplaced or stolen.
PURCHASER/RE: JESSICA COUGHLAN
AUTHORIZED SIGNATURE
VOID AFTER 90 DAYS
SECURITY FEATURES INCLUDED. DETAILS ON BACK
⑈054681⑈ ⑆312385303⑆00089235 78⑈
8.46 x 10.99 in

Real Frauds


AKDO check.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools
AKDO check.pdf
Sign In
1 / 1
99.5%
Share
AKDO
1435 STATE STREET
PO BOX 111
BRIDGEPORT, CT 06605
Bank of America
HARTFORD, CT
51-44/119
011571
011571
*FIVE HUNDRED FORTY-THREE AND 24 / 100
DATE
AMOUNT
10/19/2006
*******543.24*
PAY TO THE ORDER OF
Demetrius Mcqueen
AUTHORIZED SIGNATURE

Identity Theft Red Flags

- You get bills or CC charges for things or services you didn't buy.

  →Someone runs up bills and credit card charges in your name.
- Your bank account has withdrawals you didn't make.
- Your credit report has new accounts you don't recognize.
- You get a tax refund letter stating your refund is different than your tax return calculated.

Identity Theft – Stealing Tax Refunds

- 1 - What they need → SSN and your name.
- 2 - What they do → doctor up a phony W-2 or 1099.
- 3 - Fraudster gets refund put onto a prepaid debit card or via direct deposit into a phony account with your name on it at *their* bank (not yours).
- 4 - When you try to get your refund it is frozen by the government.
- 5 - Resolution can takes months or even years.

Identity Theft

Identity Thieves can do real damage to you beyond money!

What should you do?

Identity Theft – What do you do next?

- Report the issue to your bank/credit card issuer/IRS/State
- Close the bank or credit card account(s).
- Get new credit cards or open a new bank account.
- Report the issue to a credit reporting agency.
- Put a fraud alert on your credit report, or even a credit freeze.
- File IRS Form 14039 – "Identity Theft Affidavit."
- Report the crime to your local police.
- Go to www.IdentityTheft.gov.
- Talk to your CPA.
- Contact Social Security if your SSN has been misused.
- Change your passwords.

How to Protect Yourself from Identity Theft

- Protect your personal information.
- Shred documents before disposing them.
- Give out your SSN *sparingly*…only when absolutely necessary.
- Use strong passwords online.
- Scrutinize your monthly statements for activity you don't recognize, even the small stuff. (i.e. credit cards, bank accounts, etc.).
- Be skeptical about unusual events or communications.
- *Ask for help!*

Internet Scams – Facebook Spoofing

- You get a message from someone "*you know*"… "Check out this video. Is this you?"
  - This installs malicious software on your computer and steals your Facebook login information.
  - Call your friend and ask if they sent you the message!
  - ***Never*** click on an unknown link!
- Kidnapping Hoaxes
- Military Draft

Other Internet Scams

- Bait and switch – bogus product listing. You pay; item never arrives.
- Sales price seems too good to be true.
- Equifax Data Breach - Fake Settlement Websites.
- Iran's Cyber-attack.
- Two-factor Authentication – If you didn't sign in then it's fake!
- ***Never*** open an email (or a text message) from an unknown sender.
- Data Breaches – Change your password ASAP!
- Sign in with Facebook, Twitter or LinkedIn? Should you do this?

What Not to Put on the Internet

1. Your phone number
2. Your home address
3. Anything work-related
4. Your relationship status
5. Your birthday
6. Your payment information…don't be lazy…just enter your CC number each time you buy something online!

Other Internet Scams

- Emails Phishing Schemes – The *email looks real* but it isn't. "It looks like it's from my boss." But his account has been spoofed. *Something bad will happen*!
- Text Message Phishing Schemes – *Don't click on the link*. It's all fake. Once you enter your account information, your account is gone!

A Real Email I Received – It's a Scam!

This is the email I received from "Google":

<Sender > Security Alert <ivhdyRcNK@hstepielyczrwkuppr.com>unusual activity

Unusual activity

Someone recently used wrong passwords to try to sign in to your Google account christophergallocpa@gmail.com

we prevented the sign-in attempt, in this case please review the details of the sign-in attempt:

Monday at 08:38:12 AM UTC.

IP Address : 31.236.31.5 (GB)

NOTE : if you do not reply to this message to explain us about this unusual activity.

Our records indicate that your account will suspended , try to reply us asap.

You've Been Hacked – What to Do Next?

- *Change your password ASAP!*
- Don't log in via links sent from outside sources.
- Look for obvious mistakes in messages, such as bogus domain names, typos, etc.
- Report phishing scams to FBI Internet Crime Complaint Center (www.ic3.gov) or

Other Scams

- Ponzi Schemes ---> Bernie Madoff
- Stealing Your Tax Refund ---> Gallo's story

Password Tips

- Strong passwords are *vital*!
- Password managers can work, but not always easy to use.
  - Try “KeePass.com”
- Here’s what to do:
  1. Don’t base it on anything available to others about you.
  2. Use a phrase.
  3. Let it be long.
  4. Don’t change it until you have to.
  5. Use something memorable.
  6. Use different characters, upper-case/lower-case mix.
  7. Use two-factor authentication.

If You're Worried…Here's What You Can Do Next

- Call the FTC's Consumer Response Center…877.382.4357
- Call the IRS…800.829.1040
- File a complaint with Treasury Inspector General for Tax Administration… www.tigta.gov or call 800.366.4484
- Get your Credit Report…it's free once a year… www.AnnualCreditReport.com or call 877.322.8228
- Get more information at www.ftc.gov/PassItOn
- Subscribe to Kim Komando's Fraud & Security Alerts newsletter… www.komando.com
- Share what happened to you with your friends

Thank you for listening!

If you are having an issue…please call me.