

Identity Theft and Online Security

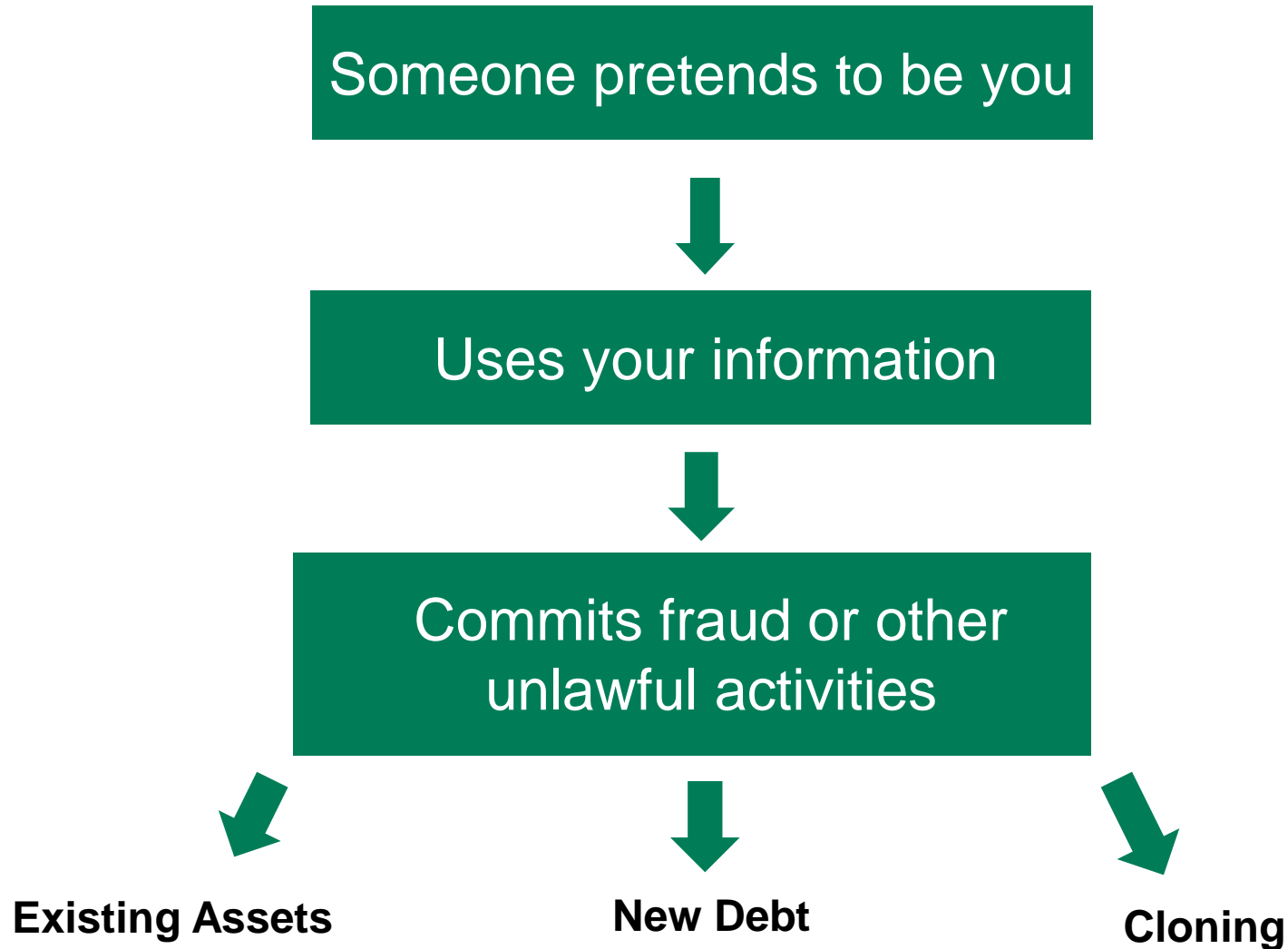
Goals for Presentation

- Identity Theft - What is it and how are we at risk?
- Social Media - How much online security do we have?
- Protection - How can we enhance our security online and make ourselves a hard target for identity thieves?

Examples of Identity Theft and Online Security

- Target Data Breach
- Pictures on Facebook

What is Identity Theft?



Interesting Facts on Identity Theft

- You have almost twice the chance of having your ID stolen as you do having your home broken into
- In more than 25% of Identity Theft cases the victim knows the thief
- When the victim knows the thief over 1/3 of the time it is a family member
- Age 29 and under is the fastest growing demographic for ID Theft
- 1/3 of robberies nationwide involve the theft of a cell phone

Favorite Targets

- **Credit Cards** – found or stolen
- **Bank Fraud** – changing amount on a check and ATM code theft
- **Utilities** – parents using child's clean credit history
- **Employment** – using someone else's social security number
- **Medical ID Theft** - most victims are age 26 to 55, and 36% of all victims reported their identification had been stolen by a family member
- **Fraudulent Tax Returns** – one of the fastest growing ID Theft crimes. Most happen early in the filing season

Accessing Your Information

Where are you at risk to have your identity stolen? Identity thieves access your personal information by many different means, including:

- Stealing your wallet or purse
- Posing as someone who needs information about you through a phone call or email
- Looking through your trash for personal information
- Stealing your mail
- Accessing information you provide to an unsecured internet site

Credit Cards and EMV Technology

- Currently you have a magnetic strip on the back of your credit card. Most other countries abandoned this technology long ago
- They have adopted EMV (Europay, Mastercard and Visa) technology – instead of a magnetic strip they have an embedded chip
- EMV chips are small computers encrypted with personal information. That information remains blocked to any card readers until a consumer enters a PIN to activate it
- As opposed to magnetic strip technology, a chip is extremely difficult to crack
- Why has US not adopted? Cash and Convenience:
 - ✓ Producing a card with the chip costs about four times as much as making a magnetic card
 - ✓ More than 8 million merchants in the US accept credit-card payments, and the terminals they use to accept those payments would all need to be updated
 - ✓ Most Americans have several cards. Remembering a PIN on one card is a challenge. But on 3-5 cards?

Social Media and Your Security

What is social media?

- Electronic communications such as websites, blogs and apps where users create communities to share information, ideas, personal messages, pictures, etc....

What is an app?

- It is an abbreviation for “application.” A piece of software that can run on your computer, laptop or phone
- In September of 2009 there were 85,000 apps at the iPhone App Store. Now there are well more than 1 million

Types of Social Media and Apps

- Facebook – I like drinking coffee with my friends
- Google – Where is a good place to drink coffee with my friends?
- Twitter – I'm drinking a coffee with my friends
- Snapchat – Here is a picture of me drinking coffee with my friends (it disappears 10 seconds after you view)
- LinkedIn – My skills include drinking coffee
- YouTube – Here is a video of me drinking coffee and spilling it
- Foursquare – This is where I drink coffee

Online Privacy and Security

Facebook, Google and social media are changing the way our world operates.

What do they know about you?

- ✓ What web sites you visit or “like” – sports teams, health conditions or treatments, sexual orientation, race, the list is often endless
- ✓ What information you search for
- ✓ Purchase history
- ✓ Geographic location
- ✓ Family members and pet names
- ✓ Email address
- ✓ Birthdate

Social media sites collect as much data as possible to help advertisers deliver ads that you may find useful.

Vast majority of this information is shared voluntarily.

Oversharing on Social Media

- Full birthdates – one of the 3 or 4 pieces of personal information that is needed to steal your identity. At least leave out the year.
- Your relationship status – stalkers would love to know that you just became newly single. It also lets them know you might be home alone. Best bet is to just leave this blank
- Your current location – the problem is you have just told everyone you are not at home
- Pictures of children tagged with their names – this is the kind of information that could be used by a predator to lure your child

Oversharing on Social Media

Who LOVES oversharing?

- Social media sites – more info to share with advertisers
- Stalkers and thieves
- Lawyers and private investigators
- Insurers, employers, and college admissions will use social media to evaluate people

Prevention and Protection - Online

Social Media Privacy Settings

- Share only with Friends – this is under “Who Can See My Stuff” in Facebook. Sharing info with “Friends of Friends” could expose your information with tens of thousands
- “Unpublic” your “Wall” - set the audience for all previous posts to just “Friends”
- Turn off “Tag Suggest” if you would rather not have Facebook automatically recognize your face in photos
- Lists – on Facebook you can create lists with a select group of people (close friends, family members, etc.....)

Facebook and other social media sites absolutely want you to share as much information as possible. As a result default privacy settings may not be in your best interests and can be very difficult to manage and comprehend.

In most cases it is a best practice to maximize your privacy settings on any social media site. Also assume anything you post on a social media site can be seen by all your family, friends, employer, health provider, and government.



Common Passwords

- Spouse, child, or pet's name, possibly followed by 0 or 1
- Last four digits of your SSN
- 123 or 1234 or 12345
- 654321
- abc123
- password
- City, college, or sports team names
- Birthdate for you, your spouse, or child

Creating a Strong Password

DO NOT USE:

- Names – pets, family members and nicknames
- Birthdates and anniversaries
- Social Security number
- Address or phone number
- College affiliations
- Sports team affiliations

Fix that password - NOW

- Build a password with at least 8-12 characters
- Contains characters from each of these categories:
 - ✓ Uppercase letters – A,B,C
 - ✓ Lowercase letter – a,b,c
 - ✓ Numbers – 1,2,3,4
 - ✓ Symbols - !@#\$%
- Create at least 3
- Store your passwords in a secure space
- Make passwords memorable without using personal data. Create an acronym or saying from an easy to remember phrase
 - ✓ YumBeet\$14
 - ✓ 21Its@WLife
 - ✓ NBigBo@t82

Phishing – Email and Phone

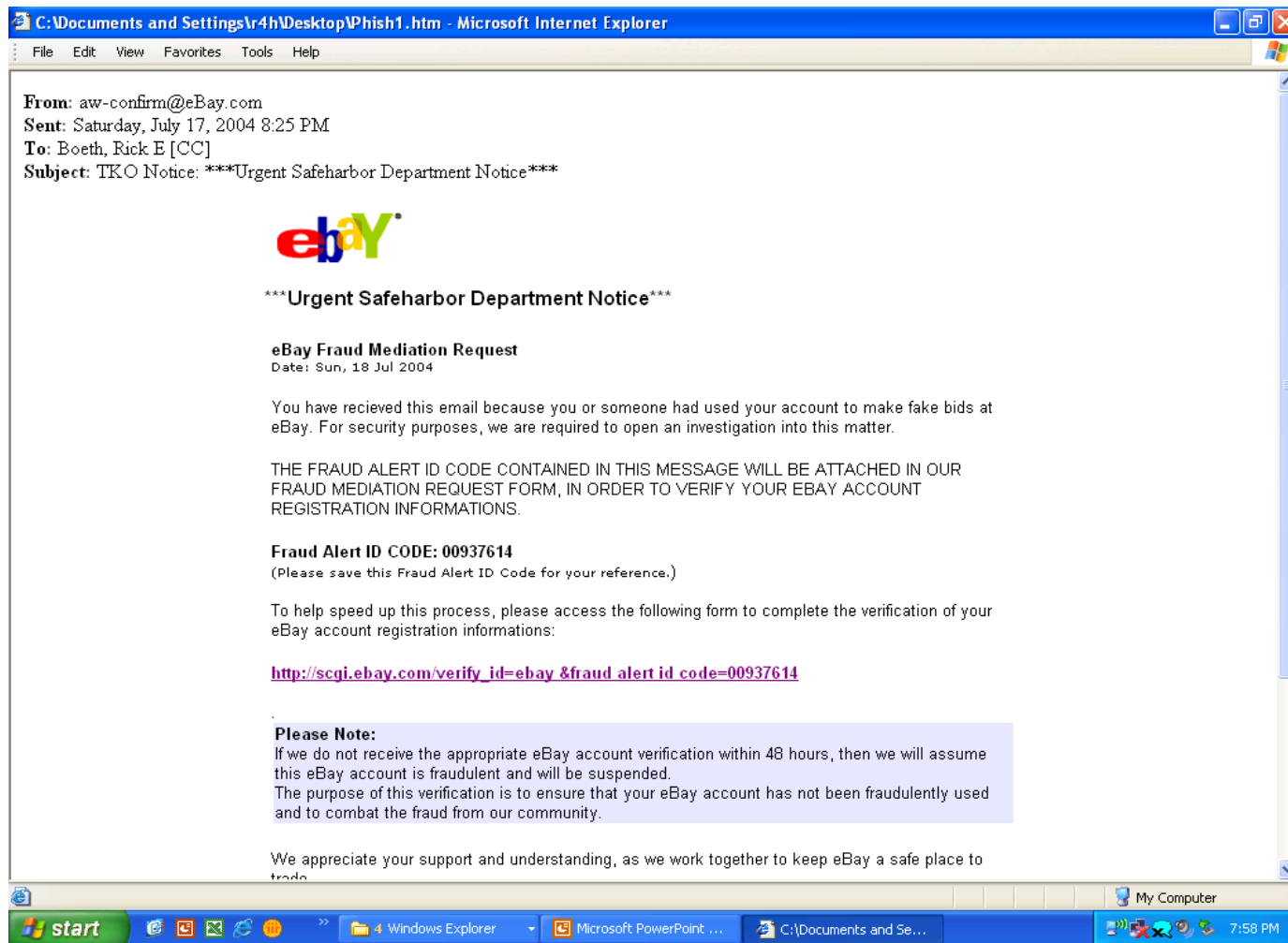
Treat ALL unsolicited requests for sensitive information with extreme caution. Here are some common characteristics used in phishing scams:

- Well known company
- Threat – “account will be closed”
- Link to a site or a phone number - NEVER click or dial
- Bad spelling and grammar


FAILSAFE – go to the company’s website and call their customer service number to see if there is actually an issue with your account. Do not trust any information in the email.

- You can forward phishing emails to phishing-report@us-cert.gov
- The IRS does not initiate contact with taxpayers by email or social media tools to request personal or financial information. If you receive a scam email claiming to be from the IRS, forward it to the IRS at **phishing@irs.gov**

Phishing – Email and Phone



Protect Your Computer

- Install an antivirus program:
 - ✓ Odds are good that when you buy a new computer it will come with security software.
 - ✓ Free programs are all that most users need
 - ✓ Well rated programs include: Avira, AVG and Avast
 - ✓ Apple computers experience fewer attacks than PCs. Their firewall and security features should offer sufficient protection
- Don't use public computers for sensitive transactions – billing, banking, etc....
- Secure your wireless network – strong password
- Look for **HTTPS://** or  when you are on a website

Be Smart With Your Smart Phone

- Lock your phone – set the four digit password and make it a strong one
- Don't save financial passwords - when you get that prompt that says "would you like to save this password for next time," do not on any financial website
- Install track and wipe software – the “Lookout” and “Find My iphone” apps are well rated
- Only download apps from trusted sources – Microsoft, Google, and Apple App stores
- Don't miss operating system updates

Traditional Prevention and Protection

What information is at risk?

- Social security number
- Birthdate
- Mother's maiden name
- Passwords
- Driver's license number
- PIN numbers
- Credit card numbers
- Bank account numbers

What is in Your Wallet/Purse?

What do you really need?

- Driver's license
- 1 credit card (possibly 2 if you use a business card)
- Debit card
- Gym card
- Work identification card
- Health insurance card

Make a front to back copy of all items and keep in secure location.

Protect Your Mail

Vulnerable information you receive:

- Telephone and utility bills
- Monthly credit card bills and bank statements
- Pre-approved credit card offers
- Pay check stubs and direct deposit receipts
- 401k and other investment statements
- Annual Social Security account statement and tax information

Make sure and stop your mail anytime you will be on vacation or away from home.

Consider investing in a cross-cut paper shredder.

Key Documents to Protect

It's best to file and store important documents in secure places such as a locking fire safe file cabinet, a home safe, a safety deposit box at your bank.

- Car title
- Birth certificate
- Social Security cards
- Tax returns (5 years)
- Insurance policies
- Deeds to property
- Loan agreements

Final Checklist

- Check your credit reports – annualcreditreport.com
- Monitor your statements: credit card, bank and medical
- NEVER give personal information in response to unsolicited emails or phone calls
- Don't leave your mail in box overnight and stop mail when you will be away
- Create strong passwords
- Set privacy controls on sites like Facebook and be very careful what information you make available online
- File your tax return as soon as possible – if you can't file early you can get a PIN number from IRS.gov.
- If you are not filing electronically hand your tax return directly to a postal employee
- Shred all sensitive information

If You Become a Victim.....

1. Close compromised accounts
2. Contact all your financial institutions immediately
3. Change your passwords
4. Contact one of the big three credit reporting bureaus and ask them to flag your information with a fraud alert. One call will place alert at all three.
 - ✓ Experian 888-397-3742
 - ✓ Equifax - 800-685-1111
 - ✓ TransUnion - 800-916-8800.
5. File a police report
6. Be sure to document everything in writing
7. Keep names and dates of everyone you speak to

Online Resources

- Microsoft safety and security system = www.microsoft.com/security
- On twitter follow “Safer online by MSFT”
- Lifelock.com
- IRS - irs.gov/uac/Identity-Protection
- FTC.gov/idtheft

American Century Investments

- **Performance focus for 55 years**
- **Pure play business model**
- **Privately controlled and independent**
- **Profits with a purpose**

The contents of this American Century Investments presentation are protected by applicable copyright and trademark laws. No permission is granted to copy, redistribute, modify, post or frame any text, graphics, images, trademarks, designs or logos.

Non-FDIC Insured – May Lose Value – No Bank Guarantee
American Century Investment Services, Inc.
©2014 American Century Proprietary Holdings, Inc. All rights reserved.

