IDENTITY THEFT

- medical records
- date of birth
- credit card numbers
- drivers license
- phone
- passport
- online
- steal

- name
- policies
- 401k
- lock
- identity
- theft
- vulnerable
- debit card
- phone
- address
- bank
- numbers
- targets
- online
- white collar
- crime

- target
- credit rating
- retirement
- savings
- websites
- computer
- sold
- bank account
- fraud
- identity theft
- medical information
- personal information
- financial information
- sensitive information
- identity thieves
- identity protection
Victims of ID theft suffer much anguish

2017 was a Record Year for ID theft in the US
16.7 million Americans fell victim

- [https://spectrum.ieee.org/riskfactor/computing/it/2017-is-another-us-record-year-in-id-information-thefts](https://spectrum.ieee.org/riskfactor/computing/it/2017-is-another-us-record-year-in-id-information-thefts)

- Identity theft takes an average of 6 months and 220 hours to resolve [http://www.identityhawk.com/identity-theft-recovery-time](http://www.identityhawk.com/identity-theft-recovery-time)
Every 19 minutes a person becomes a victim by:

- Email Phishing
- Credit/debit card information stolen at stores or restaurants by hacking or card skimming
  [https://www.youtube.com/watch?v=U0w_ktMotlo&list=PLE979CF662C9EB337](https://www.youtube.com/watch?v=U0w_ktMotlo&list=PLE979CF662C9EB337)
- Social media - Criminals use these web sites to piece together your life, contacts, work information
- Telephone scams
- Computer remote access provides cybercriminals with unlimited access to anything in your computer
Consequences

• Go to jail for someone else’s crime
• IRS notifies you more than one tax return was filed under your name
• Ruined credit
• Bankruptcy filed in your name
• Difficulty obtaining a loan or credit card
• Citations
• Rental vehicles damaged/stolen
• Student loans taken out in your name
• Higher interest rates
• Merchants refuse checks
• Debt collectors start calling your home, work, family, co-workers
• Medical Identity Theft – Thief’s medical information gets comingled with your file (blood type, allergies, illnesses)
• Refused health claims because you have reached a limit
Signs Your Identity Has Been Stolen

• A sudden increase in an account balance
• Declined credit card transaction
• Your Credit Score rating plummets
• Mysterious new account(s) within your credit report
• Debt collectors start contacting you, co-workers, family
Prevention

Teach your children as well

- Never give personal information over email/telephone/Internet web sites
- Don’t list your correct birthday on social media or PII on web site profiles
- Update anti-virus software weekly on your computer(s) and smartphone(s)
- Don’t use the same password for all user accounts
- Pick up mail in unlocked mailbox daily or use P.O. Box
- Get free credit report annually from each of 3 credit reporting bureaus. Request one free report get one every 4 months
- Place outgoing mail in secure mailbox
- Use dual authentication to sign into websites if offered
- Use fraud alert companies
Prevention, Part 2

• Opt out of pre-approved credit cards and loan offers.
  • Remove name from marketing lists of 3 credit reporting agencies and call 1-888-5-OPTOUT or go to www.optoutprescreen.com to remove you from marketing lists.
• Shred credit card offers (using a cross-cut shredder)
• Cut up expired or unused credit cards
• Review credit reports annually
• Review your bank and credit card statements at least weekly
• Never keep your SS card in your wallet or purse
• Never use a password on an unsecured Wi-Fi connection
• Ask if there are options other than providing SSN as PII
  http://blog.credit.com/2013/03/5-places-where-you-should-never-give-your-social-security-number-65328/
What to do if your identity or banking/credit card information was stolen during a data breach (e.g. Target, Home Depot, PF Changs, JP Morgan Chase)

• Security Freeze on Credit Report, small fee to initiate and remove if you need a credit check

• Protect my ID.com

• Apply for a new social security number

• Get “V” on back of your driver’s license
What to do, part 2

• Call credit reporting companies and place a fraud alert on credit reports associated with your Social Security number.
• Dispute all fraudulent charges
• Have any account that has been tampered with or opened fraudulently closed immediately.
• Contact your local police and/or the police department in the community where the identity theft took place and file a report.
• File an official complaint with the Federal Trade Commission.

The ability to act quickly can make all the difference.
Number of spam/phishing emails UNM IT blocks **DAILY**

1-3 MILLION

*If one gets through, forward to:*

- spamdrop@unm.edu
- security@unm.edu
Phishing scams

• Never disclose your financial or personal information in response to an unsolicited e-mail regardless of who sent it.
  • *If you get an email or phone call asking for personal information,* it is a scam 100% guaranteed

• Call the institution directly if you have a concern (do not call the number they provide in the email. Look it up yourself.)

• Never click on a link embedded in an unsolicited e-mail, (regardless of who sent you the email.)

• Verify the authenticity of a website before entering financial or personal information on that website
Pharming Scams

“Pharmers” redirect Internet users from legitimate commercial websites to counterfeit web pages to trick them to disclose their vital financial and personal information.
Check the URL even if you typed name in

• Always make sure the Internet web site (aka: URL) is the correct one. Hackers will sometimes register a web domain that is spelled slightly differently (e.g. swapped letters; an extended URL name)
• A secure web site must have a URL that begins with ‘https’: and display a padlock icon on the bottom page
Holding your computer hostage for money

http://krqe.com/2015/02/04/ransomware-rakes-in-millions-from-average-computer-users/

They may have already encrypted your data

Paying the ransom fee does not guarantee you will get it back or that it won’t happen again

Using your credit card only compounds your problem
Phone fraudsters recycle approach


• Calls representing IRS, threatening arrest if you don’t send money immediately. IRS does not email or call — they send you a letter

• Calls representing police departments claiming you must pay an outstanding warrant via a phone payment

• Calls stating you missed jury duty.

  Call 841-8141 to confirm your jury duty status

• Calls stating a family member has been kidnapped and they demand money for their safe return. These types of calls are made from a disposable cell.
Child/Student Identity Theft on the Rise
Goes undetected for years


• Use the child’s SSN as the family SSN due to the inability of a parent to obtain an SSN
• Pay off debt and create new lines of credit
• Avoid a criminal record on the perpetrator’s file
• Avoid a medical record with the perpetrator’s file information (perhaps for insurance purposes or to hide a medical condition)
• Fraudulently receive welfare, unemployment or medical benefits
College students on scammer’s radar

FBI warns of fictitious “Work-From-Home Scam” targeting university students

http://www.ic3.gov/media/2015/150113-1.aspx

• If a job offer sounds too good to be true, it probably is
• Never accept a job that requires the depositing of funds into your account and wiring them to different accounts
• Never provide credentials, passwords or personal information in response to a recruitment email
• Forward emails to spam@unm.edu and then warn your friends to be on the lookout for the scam
I ate Thanksgiving with my Identity Thief for 19 years

Scammed BBB president shares lessons learned


• Was closing on a Farmington building the BBB was donating to Big Brothers Big Sisters
• Received email from Big Brothers email titled “Kindly Review the Attached Document”.
• Clicked the attachment which was blank and then prompted to enter his Google email username/password.
• He complied. BIG mistake.
• Once in his email, hackers sent the identical bogus email to every email account in his address book
• Scam was designed to infiltrate friends via a trusted email account to steal personal information, bank and cc accounts
• Contained his usual signature but an incorrect phone number so if his contacts suspected something about the email, they would call a bogus phone number.
• Created an email rule so that all responding emails would go directly to the email trash can.
• Lessons learned:
  
  Do not store personal information within your email
  Do not let your guard down or logon information even if email seems to be from someone you know
The Real Threat of Identity Theft Is In Your Medical Records, Not Credit Cards

Medical identity theft carries the extra danger that errors in your medical file could lead to a misdiagnosis or mistreatment when you seek medical care in the future.

A Stolen Credit Card Is Worth $2 On The Black Market, A Stolen Medical Record? $25

• A bill for medical services you did not receive
  • A call from a debt collection agency about a medical debt you know you don’t owe
  • Medical collection notices for debts you do not owe appearing on your credit report
• A letter from your health insurance provider stating that you have reached your benefit limit when you know you have not done so, and
  • Being denied for insurance based on factors that do not apply to you

Protect Passport/CC/Cash

• RFID Blocking Wallet [https://www.youtube.com/watch?v=hcSss9BHPFo](https://www.youtube.com/watch?v=hcSss9BHPFo)

• Unless country mandates carrying passport, leave original passport in hotel safe and carry a copy in passport holders *inside* your pants

• Carry cash in money belts *inside* your pants
NM and FTC Victim Resources

http://identitytheftnetwork.org/resource-map/new-mexico

Federal Trade Commission: Step by step instructions

FBI Internet Crime Complaint Center (IC3)
If you think you have been a victim of identity theft or want further information, please contact Deb Kuidis at 277-2058 or dkuidis@unm.edu