WASHINGTON STATE UNIVERSITY EXTENSION

PROTECTING YOUR IDENTITY

WSU PEER REVIEWED

FS281E

By
Christian Koehler, Grays Harbor County Extension, Washington State University

Protecting Your Identity

Limit Access to Personal Information

Identity theft is one of the fastest growing white collar crimes. The Bureau of Justice Statistics estimates that 17.6 million persons age 16 or older were victims of identity theft in 2014 based on those surveyed, and fewer than 10% of the victims reported the incident to the police (McCarthy 2015).

Regardless of the form it takes, identity thieves need to have at least some of your personally identifiable information (PII). Some common forms of PII include your social security number, credit card and bank accounts, driver's license, utility and insurance account information, and your user names (logins), passwords, and PINs for all online accounts.

Results from the Bureau of Justice survey indicate that the majority of identity theft victims don't know how the offender obtained their information, and 9 in 10 identity theft victims didn't know anything about the offender (McCarthy 2015). Identity thieves can get your personal information in a variety of ways. There are the tried and true methods like taking the mail from your mailbox, picking through your trash, or stealing your handbag or wallet. With available technology, there are many more options for thieves like card skimmers or readers, phishing by phone, text or Internet, or other imposter scams.

You'll want to avoid opportunities for thieves to access your personal information. Carry only the identification needed. When you can, consider leaving your social security card, extra credit cards, or checkbook locked in a safe place at home rather than taking them with you. Don't write your account numbers, passwords, or PINs on your cards or slips of paper in your wallet, or sticky notes on your phone, monitor, or tablet. Always password-protect your cell phone.

Credit card skimming occurs when an identity thief attaches a "skimmer" to a credit card reader making it possible for the thief to steal and store credit card information. It's difficult to detect card skimmers attached to ATMS or point-of-sale (POS) card readers such as gas pumps. In those situations, avoid unstaffed locations, where a card skimmer could be installed and go undetected. Gas stations have until 2020 to replace magnetic strip readers with chip readers before station owners will be responsible for fraudulent purchases made with a chipped card using a strip reader. EMV credit cards with chips are more secure than cards with only magnetic strips. (EMV stands for Europay, Mastercard, and Visa, the creators of this global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.) Choose devices with chip readers whenever possible. Try to handle all transactions without handing your debit or credit card to clerks or wait staff.

Opinions vary regarding the efficacy and need for a Radio Frequency Identification (RFID)-blocking wallet, purse, or fabric. Do any of your credit or debit cards have an active RFID chip that's read without directly accessing the card reader? If not, but you still want to protect against the potential theft of your name and address from your epassport or enhanced driver's license (EDL), research products before you buy. When tested, many items did not block the RFID skimming devices.

Currently, Medicare cards have the individual's social security number printed on the front. Although the federal government will begin replacing the social security numbers with other patient identification numbers beginning in 2018, you may want to take steps to protect your social security number until you get your new card. You may want to make a photocopy of your card and blacken all but the last four numbers. If you choose to use this method, you'll need to carry a government-issued photo ID also.

Protect your incoming and outgoing mail from identity thieves. Use the post office or other secure facility to post your outgoing mail. When possible, consider a locking mailbox attached to your home for incoming mail, or rent a post office box.

Be sure to secure your phone and other electronic devices with a password, PIN, or code, as provided by the manufacturer. Choose added security when available. When selecting a password, don't use the same one for all of you accounts or devices. Create passwords that are a minimum of eight characters including upper and lower case letters, numbers, and symbols (when allowed). Do not include your user name, real name, or complete words. Some providers have guidelines associated with password selection specific to their accounts. Password experts suggest converting a sentence into letters, numbers, and symbols. You may choose to use a Password Manager software application to secure your passwords. If so, research the application. Several are available at no cost.

Be aware of personal information you share on social media sites. Learn about the privacy settings for each of your accounts and the access you're permitting. Consider the details you permit the public to see and know. Be sure that you keep your user name, password, and PIN for any sites that you access private. Don't leave them on a sticky note near your monitor, keyboard, or laptop.

Destroy Sensitive Personal Information

Can you trust everyone visiting your home? If contractors or other service providers have access to your home, be sure that any personal information is safely locked away. You may want to keep copies of paid bills for budgeting purposes and you'll want to hang onto receipts for expensive purchases. Keep these and other important papers in a secure location.

When you want to dispose of unused credit card applications, paid utility bills, etc., choose a crosscut shredder to destroy papers before disposing of them in the trash. If you live in an area that permits burning, you may find that burning paperwork in a woodstove works well for you. In many areas, local financial institutions or other businesses underwrite the cost of community mobile shredding events. You may be able to locate one near you by checking with your solid waste disposal company. Also, the Washington State Attorney General's office posts a list of events that can be found at: http://www.atg.wa.gov/community-shred-events.

Reducing the amount of junk mail that comes to your home will mean that you have less paper to shred. You should at least reduce the amount of catalogs, etc. by contacting the Direct Marketing Association at https://dmachoice.org/, or writing and requesting that your address be added to their list by mailing your request with a $1 processing fee to: DMAchoice, Direct Marketing Association, P.O. Box 643, Carmel, NY 10512. You can also contact the Direct Marketing Association to have your email added to their preference list.

Are you also inundated with credit card applications? One strategy is to opt out of credit applications by contacting OPT-OUT, operated by the major credit reporting agencies. You can choose to opt out permanently or for five years. You can contact OPT OUT by calling: 1-888-5-OPT-OUT (1-888-567-8688) (TTY: 7–1–1 and referring the Relay Operator to 1-800-821-9631) or visit www.optoutprescreen.com. If you are not interested in acquiring any new credit accounts, you can also choose to put a credit freeze on your credit report. There is usually a charge associated with this service, unless your identity has been stolen (see below).

As an extra measure, you may choose to add your landline and/or cell phone number to the Do Not Call Registry. Although this does not stop all nuisance calls, it reduces the number of legitimate telemarketing calls that you'll receive. You can do this by visiting the FTC website: https://www.donotcall.gov/ or by calling 1-888-382-1222 from the phone you want to register (TTY: 1-866-290-4236). To verify if your number is currently on the registry, visit the site or call 1-888-382-1222. Also, you can file a complaint regarding illegal sales calls or robocalls by visiting the registry or calling 1-888-382-1222 (TTY: 1-866-290-4236).

Protecting the Identity of the Deceased

If you are responsible for the estate of a deceased spouse or loved one, take steps to protect their identity. Take care not to include personally identifying information, especially birth dates and mother's maiden name, in the obituary. Report the death to Social Security by calling 800-772-1213 (TTY: 1-800-325-0778). You cannot report a death online.

It may take financial institutions and the credit bureaus a while to receive and register death records, so act promptly. Request an adequate number of copies of the death certificate so that you can provide copies for all financial institutions, credit card, mortgage and other lenders, brokerage, and insurance companies that may require one. When closing an account, request that it be closed with "Account holder is deceased". Send a copy of the death certificate by certified mail, return receipt requested to each of the credit reporting agencies and ask them to put a "deceased alert" on the person's credit report. Also periodically review the deceased's credit report for any fraudulent activity during the year.

If the individual had a driver's license or state ID card, contact the Department of Motor Vehicles to report the death. Transfer any vehicle registrations to the new owners. Also, send the IRS a copy of the death certificate so that the account will be flagged to show that the person is deceased. You can send the copy of the death certificate separately or with the individual's final income tax return. For a more comprehensive list of steps check The Identity Theft Resource Center at: http://www.idtheftcenter.org/.

Check for Evidence of Identity Theft

Carefully check bank statements and credit card and utility bills monthly. Save all receipts to verify that account charges are accurate. Be aware of your billing cycles, noting when to expect bills. Use direct deposit when possible for your IRS refund or other expected refund checks.

If you use online banking, check your account activity more frequently, particularly purchases made with your debit card. You can also call your financial institution to check account balances. Debit cards do not offer the same protection for fraudulent purchases as credit cards. You can be responsible for all unlawful withdrawals until you notify the financial institution about the error or stolen information. Your particular financial institution may provide additional protections. Be sure to read the disclosure statement provided for your account. Know your responsibility for notifying the issuer regarding fraudulent charges.

At least once a year, request a copy of your credit report from http://AnnualCreditReport.com. You can also request a copy by phone by calling (877) 322-8228, or by mail by filling out the Annual Credit Report Request form (available at AnnualCreditReport.com) and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You are entitled to receive a free copy of your credit report from each of the three credit reporting agencies: Equifax, TransUnion, and Experian every 12 months.

Regardless of how you choose to request your credit report, you have the option to request all three reports at one time or you can choose to order one report at a time. By requesting the reports separately, you can space your requests, one for each of the three companies, throughout the year. With this method you can monitor your credit more frequently.

Watch for Imposter Scams

Reports to the FTC of imposter scams jumped from less than 126,000 incidents in 2013 to 350,000 cases in 2015, and this reflects only the number of reports to the FTC. Of those 350,000 incidents reported, 228,000 — more than 65% — were IRS imposter scams (Kando-Pineda 2016, slide 80).

Identity thieves in general, but particularly imposter scams, prey on trusting and accepting individuals. The imposters contact individuals by email (phishing), phone, or in person. Regardless of how the imposter contacts the individual, the imposter will attempt to win the confidence of the victim and secure money directly, or personal information. Some common themes include dating site pickups, relatives or friends needing help, technology alerts or updates, changes in financial account information, and the very popular IRS tax return issues.

Posing as a Microsoft employee, an imposter may then ask the individual to download “antivirus software.” The imposter might connect with someone in a chat room and suggest they “take their conversation off-site,” later fabricating a story and asking for money. In the case of the IRS scam, the imposter may call, even masking their caller ID to show that the call has originated with a number having the Washington DC 202 area code. Many imposter scams depend on a sense of urgency, requesting that you take quick action, sending money or providing access to your computer or account information.

Recommendations for handling imposter scams include:

Don’t trust caller ID

Don’t send money or give out personal identification

Don’t be pressured by time

Do hang-up, delete the email, ignore texts, or close the door

Do research and check online to verify any information **independently** of the information or links provided in emails, texts, or by callers

Do call the individual, business, or organization directly

What To Do If Your Identity Is Stolen

Even when you’ve taken every precaution possible, identity theft can still occur. Thieves or their accomplices can hack into databases. Employees can steal account information and sell or use it for their own purposes. While checking your account balances or your credit report you may discover unauthorized use or charges.

If there’s a problem, contact the Federal Trade Commission at: https://www.identitytheft.gov/. This website has step-by-step instructions to create a recovery plan that you can then put into action. You can set up an account online, or browse and print the steps for a recovery plan. The step-by-step guide is also available in hard copy through the Federal Trade Commission website or can be downloaded as a PDF. The site also provides links and additional information for special situations including IRS Tax ID theft, data breaches, and medical identity theft.

You'll want to contact any of the businesses where fraudulent charges have occurred. Next, contact one of the credit reporting agencies, request a copy of your credit report and ask to have a free, 90-day fraud alert placed on your credit report. The agency you contact will contact the other two credit reporting agencies. You'll then want to file a report with your local police.

If you're a victim of identity theft in Washington State, there is no charge to request a credit freeze for your credit report. You will, however, need a copy of the police report to do so. You also need to write a letter and send it by certified mail to all three of the credit reporting agencies. State-specific details for requesting a credit freeze can be found here: http://consumersunion.org/research/security-freeze. Details from the Washington State Office of the Attorney General can be found here: http://www.atg.wa.gov/credit-freeze-fraud-alerts#fraud.

Recovery from identity theft takes time. Following the steps in the plan provided by the FTC can reduce wasted actions and help you to feel more in control.

There's always a risk that your identity can be stolen through a data breach or other third party situation. But by using these strategies, you could protect your identity and reduce the chances of identity theft.

References

AnnualCreditReport.com. 2016. All about credit reports: Getting your credit reports. Retrieved from https://www.annualcreditreport.com/gettingReports.action

Consumers Union. 2011. Security Freeze.

Direct Marketing Association. 2016. Give Your Mailbox a Makeover.

Federal Trade Commission. 2011. Stopping Unsolicited Mail, Phone Calls, and Email.

Federal Trade Commission. 2012. Fraud Alerts and Credit Freezes.

Federal Trade Commission. 2015. National Do Not Call Registry.

Federal Trade Commission. 2016. Report Identity Theft and Get a Recovery Plan.

Harrell, E. 2015. Victims of Identity Theft, 2014. Bureau of Justice Statistics.

Identity Theft Resource Center. 2017. ITRC Solution 16 Protecting Deceased's Identity.

Internal Revenue Service. 2017. Deceased Taxpayers – Protecting the Deceased's Identity from ID Theft.

Kando-Pineda, C. 2016 Identity Theft: How to Reduce Your Risk.

Kirchheimer, S. 2013. Protecting the Dead From Identity Theft: How you can safeguard your deceased loved ones — and yourself. AARP Bulletin.

McCarthy, K. 2015. 17.6 Million U.S. Residents Experienced Identity Theft in 2014. Bureau of Justice Statistics.

OptOutPrescreen.Com. 2016. Contact Us.

Washington State Attorney General. 2016. Community Shred Events.

Washington State Department of Financial Institutions. n.d. Debit Cards Frequently Asked Questions.

Washington State Office of the Attorney General. 2016. Credit Freeze and Fraud Alerts.

Washington State Office of the Attorney General. 2016. Identity Theft/Privacy.

Issued by Washington State University Extension and the U.S. Department of Agriculture in furtherance of the Acts of May 8 and June 30, 1914. Extension programs and policies are consistent with federal and state laws and regulations on nondiscrimination regarding race, sex, religion, age, color, creed, and national or ethnic origin; physical, mental, or sensory disability; marital status or sexual orientation; and status as a Vietnam-era or disabled veteran. Evidence of noncompliance may be reported through your local WSU Extension office. Trade names have been used to simplify information; no endorsement is intended. Published July 2017.