3130 Rockefeller Avenue, Everett WA 98201 ● www.Snocope.org Hours: Monday-Thursday 8:30 am-5:00 pm, Friday 8:30 am-6:00 pm ● Tel: 425-405-9973● Fax: 425-339-9482



SNOCOPE News & INFORMATION • FALL 2018



NEW SEMINAR

Cyber Security Threats -How to Protect Yourself and Your Business

October 18, 2018, 3000 Rockefeller Ave. Lower Lobby, Public Meeting Room #2 at 12 PM. Our Speaker is Grant Eckstrom, Managing Partner

Emerald City Solutions, has been providing Professional IT Support for small businesses in and around Everett, WA since 2008. They are an information security company offering high grade, Professional IT Business Solutions using cutting-edge technology to help our customers modernize their business, protect valuable assets and improve business connectivity.

Please RSVP for this FREE seminar with Beth 425-405-9983 or Email: Beth@SnoCope.org

UPCOMING EVENTS

Cyber Security Seminar - Oct. 18 Shred It Week - Oct. 15 - 19 Strides Against Breast Cancer Walk / Run - Oct. 27



Identity Theft: Protect Yourself from Predators

Defined as when one person masquerades under the identity of another, identity theft has flourished in recent years with the advent of online, faceless Internet lending and credit transactions.

Although it is almost impossible for consumers to completely guard themselves against identity theft, the Federal Trade Commission (FTC) and other consumer agencies suggest the following best practices that may help reduce the risk of loss.

• Before you reveal any personal, identifying information, find out how it will be used and whether it will be shared with others.

Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.
Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered.

• Put passwords on your credit card, bank, and phone accounts. Avoid using easily available information such as your mother's maiden name, birth date, phone number, and child's name.

Minimize the identification information and number of cards you carry to what you'll actually need.
Do not give out personal information over the phone, through the mail or via the Internet unless you have initiated the contact or know whom

you're dealing with.

• Keep items of personal information in a safe place. Be sure to tear or shred receipts, copies of credit applications, insurance forms, bank checks, and statements before disposing.

• Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home.

• Find out who has access to your personal information at work and verify that the records are kept in a secure location.

• Give out your Social Security number only when absolutely necessary. Ask to use other types of identifiers when possible.

• Don't carry your Social Security card; leave it in secure place.

• Order a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized.

• Only do business with Internet companies that use a secure form to capture private information (such as an account number or credit card number). For example, you can tell if the form is secure if the lock or key symbol on your browser status bar is solid instead of broken or open and https appears in the URL line.

• Avoid the temptation of purchasing a product from a merchant or through an auction site where the deal looks too good.

If you feel you have been a victim of identity theft, contact the FTC's Identity Theft Hotline toll-free at 1-877-IDTHEFT (438-4338); by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online. (Source: SnoCope go to http://snocope.frc.finresourcecenter.com/Avoiding_ Fraud_and_Scams_165831.html)

Identity Theft: A Survivor's Guide

Identity theft is a crime with many faces: from the thief who your skims your card info at the ATM, to the hacker who assumes your persona and opens accounts in your name. Unfortunately, rectifying identity theft damage can be like untangling a wet knot. You can do it - but it will require patience and perseverance.

2018 Holiday Calendar

NEW YEAR'S DAY OBSERVED Monday, January 1, 2018

MARTIN LUTHER KING DAY Monday, January 15, 2018

PRESIDENT'S DAY Monday, February 19, 2018

MEMORIAL DAY Monday, May 28, 2018

INDEPENDENCE DAY Wednesday, July 4, 2018

LABOR DAY Monday, September 3, 2018

VETERAN'S DAY OBSERVED Monday, November 12, 2018

THANKSGIVING DAY Thursday, November 22, 2018

DAY AFTER THANKSGIVING Friday, November 23, 2018

DAY BEFORE CHRISTMAS EARLY CLOSE 3PM Monday, December 24, 2018

CHRISTMAS DAY HOLIDAY Tuesday, December 25, 2018

NEW YEAR'S DAY Tuesday, January 1, 2019

E-mail: snocope@snocope.org

Lost/Stolen ATM/Debit Cards / 24/7 After Hours: 800-472-3272 Lost/Stolen Credit Cards / 24/7 Business Hours: 800-325-3678 Sprig Mobile Account Access: 866-698-8896 / www.getsprig.com CO-OP Shared Branching www.co-opsharedbranch.org 24-Hour Call Center: 866.692.8669 CO-OP Shared Branches/ATMs 1-888-748-3266



NMLS ID #673299





Continued from previous page Identity Theft: A Survivor's Guide.

To start, commit yourself to becoming and remaining organized. Since you will probably be communicating with a lot of people, you will need to keep track of who said what, and when. Keep copies of all letters and maintain a verbal correspondence log. File paperwork right away and store everything in a safe and accessible place.

Step One: Creditors and Financial Institutions

If accounts have been used or opened illegally, contact your creditors immediately. Ask for fraudulent transaction documentation as you may need it to file a police report. Add "non-guessable" passwords to replacement cards and all existing accounts. If a collection agency attempts to collect on a fraudulent account, explain (in writing) that you are a victim of identity theft and not responsible for the debt. Ask that they confirm in writing that you do not owe the balance and that the account has been closed. For checking account fraud, contact your financial institution to place stop payments on any outstanding checks that you did not write. Report the crime to check reporting agencies. It is also a wise idea to cancel your checking and savings accounts and obtain new account numbers and passwords. Monitor all future account statements carefully for evidence of new fraud.

Step Two: Legal and Government Agencies

Report the crime and file a report with either your local police or sheriff's department or the police where the identity theft took place. Request a copy of the report and keep the phone number of your investigator handy.

Create an Identity Theft Report with the Federal Trade Commission (FTC), which is the combination



of the Identity Theft Affidavit, also filed with the FTC, and the police report.

For additional documentation you may also pursue a Consumer Financial Protection Bureau investigation.

Notify your local postal inspector if someone else has used your address. If your social security number has been fraudulently used, alert the social security administration.

Step Three: Credit Reporting Bureaus

The most arduous task in this process may be ensuring that your credit report lists only factual information. To know what is being reported, you will need to obtain a credit report from each of the three major credit bureaus (if you are married, your spouse should also check his or her report). Even if the fraudulent information hasn't yet appeared on your credit reports, be proactive and report the crime now. Contact one of the bureau's fraud department and request that an extended fraud alert be entered on your file for seven years instead of the normal 90-180 days. Confirm that the bureau you filed the fraud alert with will contact the other two bureaus for you and have them place the fraud alerts.

Write a victim's report - a brief statement describing the details of the crime - and send it to the bureaus to be added to your credit report. The first credit reports with the fraud alert are free and will be sent to you automatically. After that, check your credit report every three months to ensure accuracy.

Healing the wounds of identity theft will take time and work. However, the sooner and more aggressively you deal with the problem, the faster you will see results. (Source: Revised January 2016, from Balance. https://snocope.balancepro.org/resources/articles/identity-theft-survivors-guide)

Did you know SnoCope has Legal Advice & Identity Theft Protection through LegalShield? You can find the info on our website under the Member Perks tab, go to Deals and Discounts.

• Identity Theft Detection and Resolution - ID-Shield protection provides you valuable services from detection to resolution. You'll feel empowered knowing that for a small monthly fee you have the expertise you need to help protect yourself against identity theft and resolve issues related to it.

• Expert Advice - After you become a member and if you have questions or concerns related to identity theft, just call the number on your IDShield member card to speak to an expert who can answer questions and take over the restoration process for you.