



Seldovia Gazette

Serving Seldovia, Alaska and Kachemak Bay southeast

Seldovia, AK

46 °F / 8 °C

Light Rain
at 12:53 AM

Advisory! 
Click for Forecast

Thursday, Sep. 30, 2010

Just another day in paradise

Local News

Calendar

Opinions

Spotlight

School

Classifieds

Archives

Seldovia.com

Gazette Services

Our Local Police Report

Submitted by Andy Anderson - Seldovia Chief of Police

PO Box 85, Seldovia, Alaska 99663

Office # 907-234-7640 Fax # 907-234-7883

Email: selpd@xyz.net

Call 911 for emergencies or assistance

No current report available as of September 1, 2010

Tips From Andy...

The "Tips from Andy" are provided as information, to our citizens and friends to be alert to potential situations that may arise. Both the Chief and I have checked on the reliability of the advice through sources like Google, BreakTheChain, Hoax-Slayer or Snopes, etc. But it is important to note, that even with the checking of this information, we are relying on the truth of yet another internet source.

Jury Duty Scam

Alaska State Troopers are warning the public against a scam hitting the nation aggressively pursuing identity theft through jury duty summons.

The caller claims to be a jury coordinator and states that you failed to show up for jury duty. If you protest that you never received a summons for jury duty, the scammer asks you for your Social Security number and date of birth. The caller claims they need the information to check their system for an error and so the fictitious arrest warrant can be cleared. **DO NOT COMPLY!!!** By providing the caller with your personal information, you become the victim of identity theft.

Most of us take summonses for jury duty seriously, but enough people skip out on their civic duty that this new scam has surfaced. This scam has been reported in 11 states. The scam is particularly insidious because the callers pretend to be with the court system and use intimidation tactics over the phone to try to bully people into giving information. The FBI and the federal court system have issued nationwide alerts on their web sites, warning consumers about the fraud.

Keeping Records Safe

[Click Here to Go Directly to Social Security Online Website](#)

[Click Here for Article about Keeping Your Records Safe - Jean Chatzky](#)

[A Letter From A Corporate Attorney To The Employees of His Company](#)

1. Do not sign the back of your credit cards. Instead, put 'PHOTO ID REQUIRED.'
2. When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the 'For/Memo' line. Instead, just put the last four numbers. The credit card company knows the rest of the number, and anyone who might be handling your check as it passes through all the check processing channels won't have access to it.
3. Put your work phone # on your checks instead of your home phone. If you have a PO Box use that instead of your home address. If you do not have a PO Box, use your work address. Never have your SS# printed on your checks. (DUH!) You can add it if it is necessary. But if you have it printed, anyone can get it.
4. Place the contents of your wallet on a photocopy machine. Do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. I also carry a photocopy of my passport when I travel either here or abroad. We've all heard horror stories about fraud that's committed on us in stealing a Name, address, Social Security number, credit cards. In case your luggage is lost, take another list in your carry on bag, especially if you are abroad and need immediate access to those numbers.

Unfortunately, I, an attorney, have first hand knowledge because my wallet was stolen last month. Within a week, the thieves ordered an expensive monthly cell phone package, applied for a VISA credit card, had a credit line approved to buy a Gateway computer, received a PIN number from DMV to change my driving record information online, and more. But here's some critical information to limit the damage in case this happens to you or someone you know:

5. We have been told we should cancel our credit cards immediately. But the key is having the toll free numbers and your card numbers handy so you know whom to call. Keep those where you can find them.
6. File a police report immediately in the jurisdiction where your credit cards, etc., were stolen. This proves to credit providers you were diligent, and this is a first step toward an investigation (if there ever is one).

But here's what is perhaps most important of all: (I never even thought to do this.)

7. Call the 3 national credit reporting organizations immediately to place a fraud alert on your name and also call the Social Security fraud line number. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the Internet in my name. The alert means any company that checks your credit knows your information was stolen, and they have to contact you by phone to authorize new credit.

By the time I was advised to do this, almost two weeks after the theft, all the damage had been done. There are records of all the credit checks initiated by the thieves' purchases, none of which I knew about before placing the alert. Since then, no additional damage has been done, and the thieves threw my wallet away this weekend (someone turned it in). It seems to have stopped them dead in their tracks.

If you are willing to pass this information along, it could really help someone that you care about.

BEWARE - New Credit Card Scam

Snopes.com : <http://www.snopes.com/crime/warnings/creditcard.asp>

About.com: http://urbanlegends.about.com/library/bl_credit_card_fraud.htm

This one is pretty slick since they provide YOU with all the information, except the one piece they want.

Note, the callers do not ask for your card number; they already have it.. This information is worth reading. By understanding how the VISA & Master Card Telephone Credit Card Scam works, you'll be better prepared to protect yourself.

One of our employees was called on Wednesday from 'VISA', and I was called on Thursday from 'Master Card'.. The scam works like this: Caller: 'This is (name), and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for \$497.99 from a Marketing company based in ?'

When you say 'No', the caller continues with, 'Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from \$297 to \$497, just under the \$500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?'

You say 'yes'. The caller continues - 'I will be starting a Fraud investigation. If you have any questions, you should call the 1- 800 number listed on the back of your card (1-800 -VISA) and ask for Security.'

You will need to refer to this Control Number. The caller then gives you a 6 digit number. 'Do you need me to read it again?'

Here's the IMPORTANT part on how the scam works. The caller then says, 'I need to verify you are in possession of your card'. He'll ask you to 'turn your card over and look for some numbers'. There are 7 numbers; the first 4 are part of your card number, the next 3 are the security Numbers that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card. The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, 'That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?' After you say No, the caller then thanks you and states, 'Don't hesitate to call back if you do, and hangs up.

You actually say very little, and they never ask for or tell you the Card number. But after we were called on Wednesday, we called back within 20 minutes to ask a question. Are we glad we did! The REAL VISA Security Department told us it was a scam and in the last 15 minutes a new purchase of \$497.99 was charged to our card.

Long story - short - we made a real fraud report and closed the VISA account. VISA is reissuing us a new number.**What the scammers want is the 3-digit PIN number on the back of the card.** Don't give it to them. Instead, tell them you'll call VISA or Master card directly for verification of their conversation. The real VISA told us that they will never ask for anything on the card as they already know the information since they issued the card! If you give the scammers your 3 Digit PIN Number, you think you're receiving a credit. However, by the time you get your statement you'll see charges for purchases you didn't make, and by then it's almost too late and/or more difficult to actually file a fraud report.

What makes this more remarkable is that on Thursday, I got a call from a 'Jason Richardson of Master Card' with a word-for-word repeat of the VISA scam. This time I didn't let him finish. I hung up! We filed a police report, as instructed by VISA. The police said they are taking several of these reports daily! They also urged us to tell everybody we know that this scam is happening. Please pass this on to all your family, friends and neighbors. By informing each other, we protect each other.

Good Advice about emails

A friend who's a computer expert received the following from a system administrator for a corporate system. It is an excellent message that absolutely applies to all of us who send emails. Please read the short letter below, even if you're sure you already follow proper procedures. Do you really know how to forward emails? Only 50% of us do.

Do you wonder why you get viruses or junk mail and hate it? Every time you forward an email there is information left over from the people who got it before you. Namely their email addresses and names. As the messages get forwarded along, the list of addresses build and build, until all it takes is for some poor sap to get a virus and his/her computer can send that virus to every email address that has come across his computer. Or, someone can take all of those addresses and sell or send them junk mail in the hopes that you'll go to the site and he'll make five cents for each hit. That's right, all of that inconvenience over a nickel! How do you stop it? There are several easy steps. Try the following if you aren't doing it already:

(1) When you forward an email, delete all of the addresses that appear in the body of the message (at the top). That's right, delete them. Highlight them and delete them, backspace them, cut them, whatever it is you know how to do. It only takes a second. You must click the 'Forward' button first and then you will have full editing capabilities against the body and headers of the message. If you don't click 'Forward' first, you won't be able to edit the message at all.

(2) Whenever you send an email to more than one person, do not use the To: or Cc: fields for adding addresses. Always use the BCC: (blind carbon copy) field for listing the addresses. This way the people you send to will only see their own email address. If you don't see your BCC: option click on where it says To: and your address list will appear. Highlight the address and choose BCC and that's it, it's that easy. When you send to BCC your message will automatically say 'Undisclosed Recipients' in the 'TO:' field of the people who receive it.

(3) Remove any 'FW ' in the subject line. You can rename the subject if you wish or even fix spelling.

(4) Always hit your Forward button from the actual email you are reading. Ever get those emails that you have to open 10 pages to read the one page with the information on it? By Forwarding from the actual page you wish someone to view, you stop them from having to open many emails just to see what you sent.

(5) Have you ever gotten an email that is a petition? It states a position and asks you to add your name and to forward it to 10 or 15 people or your entire address book. The email can be forwarded on and on and can collect thousands of names and addresses. A FACT: The petition is actually worth a couple of bucks to a professional spammer because of the wealth of names and addresses contained there. Do not put your email address on any petition. If you want to support the petition, send it as your own personal letter to the intended recipient. Your position may carry more weight as a personal letter than a laundry list of names and addresses on a petition. (And don't believe the ones that say that the email is being traced, it just ain't so!)

Some of the other emails to delete and not forward are:

1. The one that says something like, 'Send this email to 10 people and you'll see something great run across your screen.' Or sometimes they'll just tease you by saying 'some-thing really cute will happen.' IT AIN'T GONNA HAPPEN! (We're still seeing some of the same emails from 10 years ago!)

2. I don't let the bad luck ones scare you, they get trashed.

3. Before you forward an 'Amber Alert', or a 'Virus Alert', or some of the other emails floating around now-a-days, check them out before you forward them. Most of them are junk mail that's been circling for YEARS! Just about everything you receive in an email that is in question can be checked out at Snopes. Just go to www.snopes.com. It's really easy to find out if it's real or not. If it's not, don't pass it on.

Another way to check if a real virus exists is to pull up Google as a web browser and type in the title of the suspect virus, ie: mad cow virus, then enter it. Google will display a number of sources that will verify it as a virus or as a hoax.

So please, in the future, let's stop the junk mail and the viruses and be a good email neighbor.

Copyright © 2010 Seldovia.com and Seldovia Gazette. All rights reserved. Contents of this publication may not be used or reproduced, in whole or in part, in any form or manner without the express written permission of Seldovia.com