

LEARN HOW TO REDUCE YOUR RISK OF FRAUD

AVOID IDENTITY THEFT

All that a thief needs is your name, address, and social security number to steal your identity.

A thief can easily obtain this information, but there are specific things you can do to protect yourself from becoming a victim.

If you don't already have one, get a paper shredder. Use it for any



mail you dispose of that contains any sensitive information. Many times culprits obtain your information by rummaging through your trash.

Another thing you could do is obtain a credit report once a year from all three credit reporting agencies and make certain there are no inaccuracies. If there are any, report them immediately. To receive your credit report, go to www.annualcreditreport.com on the internet.

Read your account and credit card statements as

soon as they arrive and check for unauthorized transactions. If your bills don't arrive on time, notify your creditors. Many times a culprit will do a "change of address" to divert your mail and important information to them.

Unless absolutely necessary, do not divulge your social security number to anyone. Also, do not carry your social security number in your wallet or purse in case it is lost or stolen.

Photocopy both sides of your driver's license,

ATM, credit, debit and health insurance cards and keep them in a very safe place. You'll have all the information you need to notify creditors to stop charges on your accounts in case your wallet or purse is stolen.

Also, regularly update your antivirus software and don't download files sent by strangers.

Do not click on hyperlinks from email senders you don't know. Even if it looks like a legitimate site, it could be a hacker trying to steal your information.

CELL PHONE AND TEXT MESSAGE SCAMS

Cell phone users should be wary of unsolicited text messages. Recently, a number of members have received unsolicited text messages, claiming to be from their financial institution. The text urges the recipient to call a number provided for information about account discrepancies and then solicits individual account information and pin numbers.

CU Hawaii will never send you a text regarding your account information. If you should receive

a text claiming to be from your financial institution, immediately delete and do not respond to the text message.

All deleted text messages should be removed. The perpetrators have been known to use Spyware in conjunction with their text message solicitation, which can be used to intercept or take partial control over your phone's computer system if the messages are not completely removed from your phone.

We also suggest contact-

ing your cell phone provider to inform them of the situation.

There have also been cases where members have received calls claiming to be from VISA.

They state that because of your good relationship, they would like to send you a \$50 gift card; however, there is a \$2 processing fee and they need you to verify your account information. Never provide your personal information in response to an unsolicited request whether over the phone or online. If you

believe the contact may be legitimate, contact the institution yourself from the numbers provided on your monthly statements or the numbers on the back of your credit/debit cards.

Please notify CU Hawaii if you receive an unsolicited request for account information whether over the phone, online or through a text message.



UNAUTHORIZED DEBIT/CREDIT CARD ACTIVITY

As the use of your debit/credit card increases, so does the chance for fraud.

Recently, an unusually large volume of unauthorized debit and credit card activity has been occurring in the states of:

- Florida

- Georgia
- Illinois
- Texas

To minimize fraud losses, CU Hawaii may be implementing certain card restrictions in certain states or from certain merchants.

Please notify CU Hawaii at (808) 933-6700 if you plan on traveling to these destinations, if you detect any unauthorized activity or if you should be experiencing debit or credit card authorization problems.



“PHISHING” SCAMS

“Phishing” is a new type of internet piracy. It is pronounced “fishing” and that is exactly what these thieves are doing, “fishing” for your valuable personal information.

In a typical case, you’ll receive an e-mail that may appear to come from a reputable company that you recognize and do business with.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases like, “immediate attention required” or “Please contact us immediately regarding

your account”.

The e-mail will then encourage you to click on a link to go to the institutions website.

In a “Phishing” scam, you could be redirected to a phony website that may look exactly like the real thing. Sometimes, it may be the company’s actual website. However, the thieves have inserted a pop up window that will immediately appear for the purpose of harvesting your personal information.

You may be asked to

update your account information for verification with your social security number, your account number, your password, mother’s maiden name, or place of birth.

They want any confidential information that they can use to loot your accounts or run up bills on your credit cards. In the worst case you could find yourself a victim of identity theft.

To protect yourself from “Phishing” scams, never provide your personal information in response to an unsolicited request whether over the phone or online.

If you believe the contact may be legitimate, contact the institution yourself from the numbers provided on your monthly statements or the numbers on the back of your credit/debit cards.

Never provide your password or confidential information over the phone or in response to an unsolicited email request.

A financial institution would never ask you to verify your account information online. Beware of phishing scams and know how to protect yourself and your finances.



They're phishing
for you

don't bite

CHECK SCAMS

While scammers increasingly turn to the Internet, consumers are still targets of check scams.

During a five-month period from January to June 2004, check scams collected an average \$5,000 loss per consumer.

There are several variations of the check scam. The most common strategy is the "Nigerian Advance Fee Fraud," with

100 victims daily.

The scammer proposes to send the victim a check for an extra sum and requests the victim wire back the excess money. The scammers claim to be from other countries, which explains why it is too difficult for them to make direct payment.

Scammers offer you a sweepstakes you won or pay you to work at

home.

Victims often send the product or money to the scammer once they receive payment. However, the realistic looking checks sent to victims are forgeries and, unfortunately, the victims are responsible for the money they withdraw against the bad check.

Experts advise to not send refunds or deliver



goods in the period it takes cashiers' checks to clear.

ATM SCAMS

Scammers who target ATM users use the latest technology to their advantage.

The newest ATM scam involves skimming. A skimmer is a card-swipe device that reads the information on a consumer's ATM card.

Fraudsters make counterfeit ATM cards that en-

code all the information from an ATM card when they swipe immediately after the machine's last transaction.

A small camera is mounted on the ATM, which catches the PIN (personal identification number) of each user.

The consumer is unaware they've been scammed

because the ATM card has not been stolen and still works at other machines.

Many people fall victim to these crimes because their card is never stolen and they only detect a problem when they notice their

account balance is down.

The "Lebanese Loop" is another popular ATM scam. Scammers insert a portable steel loop into an ATM card slot. The scammer usually approaches the victim while at the machine, and poses as the person next in line.

Victims are advised to enter their PINs three times and then hit cancel to get the machine to accept the card.

The scammer is able to memorize the PIN for future use and the machine keeps the card because of the excessive number of attempts to enter the correct PIN.

Victims leave in frustration because they couldn't get any money

and they've lost their card.

Once the loop is taken out of the ATM the scammer has the card and the PIN number for future transactions.

This is a relatively new scam that many experts believe will be short-lived due to fast technology upgrades.

While it is difficult to guarantee protection from ATM scammers, there are security tips that lessen the risk.

Be on the lookout for anything out of the ordinary at the ATM, such as odd-looking equipment or wires.

As always, monitor your accounts regularly to make sure there is no unusual activity.

