

Protect yourself from financial fraud

Consumers are increasingly at risk of being victims of financial crimes. Armed with as little information as a Social Security Number, crooks can steal an individual's identity and apply for credit in his or her name. Another relatively new concern is the use of "skimming" devices, which allow a thief to steal a card's magnetic stripe and keypad information from ATM machines and gas pumps.

Moreover, with the growth in Internet transactions and e-mail use, there are new types of scams popping up every day. One scam growing in frequency is called "phishing." In this case, con artists use email to try to hijack a person's financial information. In a phishing scam, swindlers claim to be from a reputable company and send out thousands of fake emails in hopes that consumers will respond with the bank account information, credit card numbers, passwords or other sensitive information.

These emails can look quite convincing, with company logos and banners copied from actual Web sites. Often, they will tell the recipient that their security procedure has changed or that they need to update (or validate) the recipient's information. The consumer is then directed to a look-alike Web site that, if the consumer responds, will provide the thief with personal financial information they will then use to order goods, services or obtain credit.

To avoid "phishing" scams, consumers should consider the following tips:

-Never give out your personal financial information in response to an unsolicited phone call, fax or email, no matter how official it may seem.

-Do not respond to email that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the email's validity using a telephone number or Web address you know to be genuine.

-Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.

-When submitting financial information to a Web site, look for the padlock or key icon at the bottom of your browser and make sure the Internet address begins with "https." This signals that your information is secure during transmission.

-If you have responded to an email, contact your bank immediately so they can protect your account and your identity.

Another extremely common scam that has been around for decades involves an offer- now commonly received via e-mail- from supposed Nigerians kindly promising big profits in exchange for help moving large sums of money out of their country. Many consumers are continuing to fall for the convincing sad stories, polite language and the unequivocal promises of money. These advance-fee solicitations are scams and according to the Federal Trade Commission, the scam artists are playing each and every consumer for a fool through their elaborate scheme.

If you're tempted to respond to an offer, the Federal Trade Commission suggests you stop and ask yourself two important questions: Why would a perfect stranger pick you- also a perfect stranger- to share a fortune with and why would you share your personal or business information, including your bank account numbers or your company letterhead, with someone you don't know?

If you receive an offer via email from someone claiming to need your help getting money out of Nigeria- or any other country, for that matter- forward it to the Federal Trade Commission at spam@uce.gov.

While there are several other pitfalls not specifically mentioned here, the basic tips for protecting our financial information apply across the board.

Get a copy of your credit report from each of the three major credit bureaus: TransUnion 1 (800) 888-4213; Equifax 1 (800) 685-1111; and Experian 1 (888) 397-3742, to check for accuracy.

Keep an eye on your accounts throughout the year by reading your monthly/periodic statements thoroughly. That's an easy way for you to be sure that all of the activity in your accounts was initiated by you.

Tear up or shred pre-approved credit offers, receipts and other personal information that link your name to account numbers. Don't leave your ATM or credit card receipt in public trash cans. Crooks (a.k.a. dumpster divers) are known to go through trash to get account numbers and other items that will give them just enough information to get credit in your name.

If your credit card or other bills are more than two weeks late, you should do three things: First, contact the Postal Service to see if someone has forwarded your mail to another address. Second, contact your bank to ask if the statement or card has been mailed. Third, contact the businesses that send you bills.

When you pay bills, don't put them in your mailbox with the red flag up. That's a flashing neon light telling crooks to grab your information. Use a locked mailbox or the post office.

Protect your account information. Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your social security number or credit card account number on a check. Cover your hand when you are entering your PIN number at an ATM.

Don't carry your Social Security card, passport or birth certificate unless you need it that day. Take all but one or two credit cards out of your wallet and keep a list at home of your account information and customer service telephone numbers. That way, if your wallet is lost or stolen, you'll only have to notify a few of your creditors and the information will be handy.

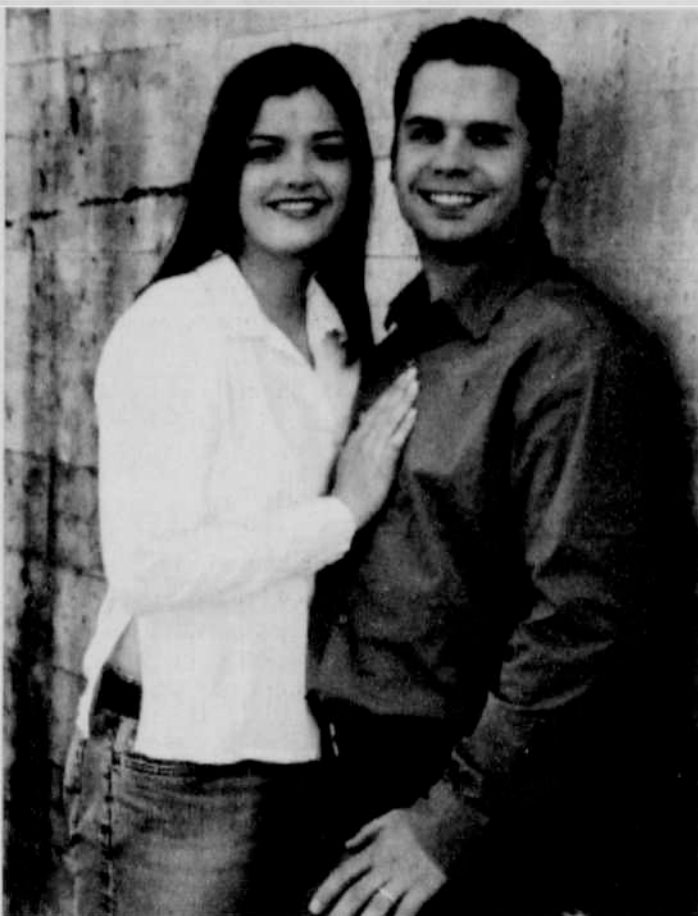
When shopping online, be sure the site is secure and reputable. Just because a site says it is secure doesn't mean it is. Be cautious purchasing from sites that advertise to be companies with no known physical address.

Never provide personal or credit card information over the phone, unless you initiated the call. Crooks are

By George Koffler President and CEO, Bank of Eastern Oregon

known to call with news that you've won a prize and all they need is your credit card number for verification. Don't fall for it. Remember the old saying, "If it sounds too good to be true, it probably is."

Engagement Elguézabal-Payne



Petra Elguézabal and Kevin Payne

Kevin Payne and Petra Elguézabal wish to announce their engagement and forthcoming marriage. The couple plans to wed on June 11, 2005, at Our Lady of Angels Catholic Church in Hermiston.

The bride-elect is a 1998 graduate of Heppner High School and presently teaches Spanish at Heppner High School. She is the daughter of Mary Ann Elguézabal of Heppner and the late Juan Elguézabal.

The groom-elect is a 1994 graduate of Heppner High School and currently works for the Oregon Department of Fish and Wildlife. He is the son of Les and Kathy Payne of Umatilla and Phyllis and Jerry Armitage of Wenatchee, WA.

Chamber of Commerce Luncheon time for awards and installation of officers



New board members of the Heppner Chamber of Commerce were sworn in last week at the annual Chamber of Commerce Luncheon. Left to right are: Bert Houweling, Jeff Bailey, Barbara Hayes, David Sykes, Nancy Snider, Tim Van Cleave, Nancy Gochnauer (Chamber President), Brenda Sherrell and John Murray.



Dale Bates received one of the "Hats Off" awards for his community service work especially helping with the sound systems at many local events.

The Heppner Chamber of Commerce held its annual luncheon last Tuesday at the Episcopal church. Awards were handed out and 2005 board members were sworn



Incoming chamber president Nancy Gochnauer presents 2004 president Victor Dose with a plaque for his service to the community.

in. Incoming president Nancy Gochnauer said she would like to see the Chamber do more to help the youth in the community in 2005.

Six HHS football players named to All-State teams



(L-R):Rory Kilkenny, Brandon Seitz, and Matt Kenny, all named to positions in 2A All-State football.



(L-R): Kory Paullus and Tyler Boyer, also named to positions in 2A All-State football. Not pictured: Jode Coil.

Six Heppner High School football players were named to positions in 2A All-State football. Those listed were: Brandon Seitz, a HHS senior, was named to the 2A All-State football second team for both offense and defense. He was chosen as a tight end and a defensive lineman.

Rory Kilkenny, a HHS junior, was named to the second team as an offensive

lineman and to the third team as a defensive lineman.

Senior Kory Paullus rounded out the HHS players named to the second team with his position as a defensive back. Seniors Jode Coil and Tyler Boyer were both named to the third team, with Coil as a defensive back and Boyer as a running back.

Junior Matt Kenny received an honorable mention as a linebacker.



Larry Mills was given a "Hats Off" award by Claudia Hughes for his many years of service to the community