



State of Nevada Department of Business & Industry

Director's Office

555 East Washington Avenue, Suite 4900
Las Vegas, Nevada 89101
Phone (702) 486-2750 | Fax (702) 486-2758
dbi.state.nv.us

FOR IMMEDIATE RELEASE — November 7, 2008
CONTACT: Elisabeth Shurtleff, Public Information Officer
PHONE: (702) 486-2756 E-MAIL: eshurtleff@business.nv.gov

Consumer Affairs Warns: Throw This Phish Back!

Las Vegas — The Nevada Consumer Affairs Division is alerting consumers to watch out for Phishing scams, an insidious type of scheme that hits consumers where it hurts the most: their finances.

“In this troubled economic climate, we are seeing a resurgence of financial scams,” says Consumer Affairs Commissioner James E. Campos. *“Phishing scams - cons in which thieves steal consumers’ personal identity data and financial account information using phony e-mail messages or websites - are on the rise, and we don’t want Nevadans to get caught in that net.”*

Phishers typically target online bankers. The scam usually works like this:

- A customer receives an e-mail message that looks like it’s from their bank.
- The e-mail requests updated personal information, such as passwords or credit card data, and the message includes a link.
- The link seems seem to go to the customer’s bank, but instead takes the customer to a phony site created by scammers trying to access the customer’s bank accounts or credit cards.

-more-

Commissioner Campos adds, *“This is an extremely devastating scam, but there are ways that consumers can protect themselves.”* According to the [Anti-Phishing Working Group](#), there some basic precautions consumers can take to make sure they don’t become victims of this crime.

- Be wary of email messages containing urgent requests for personal financial information.
- If you don’t know the sender or something looks off, don't use the links in an e-mail or instant message.
- Don’t fill out forms in e-mail messages that ask for personal financial information.
- Make sure you’re using a secure website when you submit credit card data or other personal information.
- Check your online accounts regularly.
- Check your bank, credit and debit card statements for accuracy.
- Check your credit report to see if accounts have fraudulently been opened in your name.

If you’re a victim of Phishing, don’t hesitate to take action. First, forward the phony e-mail to the appropriate authorities: reportphishing@antiphishing.org and the Federal Trade Commission at spam@uce.gov. Always include the entire original email with its original header information intact when you forward the message. Second, contact the three credit bureaus and ask them to place a fraud alert on your account. Finally, contact The Internet Crime Complaint Center of the FBI by filing a complaint on their website at <http://www.ic3.gov/default.aspx> as well as your local enforcement agency.

Fore more information, visit <http://www.antiphishing.org/index.html>. In addition, Commissioner Campos encourages consumers to visit the Fight Fraud Website at <http://fightfraud.nv.gov/>. *“The site includes extensive tips on how to prevent fraud and provides downloadable complaint forms to help you respond effectively if you become a victim,”* says Campos. *“Visit it regularly for the latest fraud alerts.”*

-END-