D.L. Evans | BANK

What is Phishing?

The term 'Phishing' (pronounced 'fishing') is a slang IT word, made up by replacing the letter 'f' with 'ph.'

Phishing, is exactly that, fishing for information - usually personal information such as credit card, bank account, or social security numbers.

Scammers 'Phish' for your personal information in a variety of ways, but most commonly through fraudulent emails claiming to be from your bank or another institution that already has your personal details, asking you to confirm these details.

Once scammers have 'phished' out your information, they could use it in a number of ways. Your credit card could be used for unauthorized purchases, your bank account could be cleared out, they may simply gather the information for an identity theft scam, or they may sell your information to identity theft rings.

Phishing emails are commonly used in association with a fake web site that looks very similar to a real website from the relevant institution.

Please visit www.fraudwatchinternational.com for examples of phishing emails.

Important Information
D.L. Evans Bank will not request personal or sensitive information (full Social Security Number, passwords, full Debit/Credit Card Number, or PINs) when contacting you. However, D.L. Evans Bank or our authorized Fraud Department may contact you regarding suspicious transactions on your account and request information to verify your identity. If you are suspicious of these automated phone calls, you are welcome to call us to ensure the phone call was indeed valid. We can be reached at 208-678-2552 or 1-866-661-5463, Monday through Friday from 8:00 am – 5:00 pm.