Scams: What's Common and How to Avoid Them

Crooks are continually trying to steal people's private information using bogus emails, websites, phone calls, and texts. They use a variety of tactics to attempt to persuade people into giving out their Social Security numbers, bank account numbers, and other private information. Most of the time, the criminal's goal is to steal money from you. This handout will go over terms used as well as ways to prevent you from falling victim to these scams.

Common Scams

Government Imposter Scams – This is when scammers pretend to be an employee of the IRS or other government agency to try to gain personal information. Sometimes the fraudsters even use real employee names after doing some simple research.

Remember that government agencies do not send spontaneous communication asking for money or private information. No government agency will ever require you pay by wiring money, gift cards, or digital currency.

Lottery or Sudden Riches scams – This is when scammers tell you that you've won a lottery or that you're entitled to inheritance from a distant relative or situation of which you've not been aware. Often, they tell you that you'll need to pay the taxes or fees on the lottery winnings or inheritance and send a fake cashier's check requesting you send the "taxes and fees" back to them. After the money is sent, the check is found to be fraudulent and the bank will then hold you responsible for the full amount, leaving you out any money you sent them or spent from the check.

Online Auctions, Classified Listings, and Overpayment Scams – This involves an online auction or classified listing site. The fraudster contacts you wanting to buy something you have listed and send a check for more than what the agreed upon amount for the item was. When it is pointed out to them, they tell you it was in error and then request that you send the amount above the agreed upon amount back to them. In a similar fashion as a Lottery Scam, the check is then found to be fraudulent and the bank will then hold you responsible for the full amount.

Grandparents Scams – This is when scammers contact you pretending to be a relative or grandchild stranded abroad or requiring money urgently to get home or for other pressing needs. They often request credit card information or a wire transfer to get the money to them quickly. If you do receive such communications, make sure you verify it is the relative they are claiming to be by contacting the individual through means you know are valid before sending any money or private information.

Secret or Mystery Shopper Employment Scams – In this scam, an ad may be placed or emailed advertising an employment opportunity to work from home. The scammer then sends a fake check as a sign on bonus and asks that you cash the check and send back funds to activate your account. The fraudster's hope is that you'll send the money before it is discovered that the check is bad. In the Mystery Shopper Employment Scam, it may ask that you "mystery shop" money transfer businesses. The fraudster sends a check, asking you to cash it and send the funds via a money transfer business and then asks that you rate the business and service you received. The check is then returned as fraudulent, and the scammers get the money that was transferred.

How to Avoid Scams

Before providing any personal information, verify that the email, text message, or voicemail is legitimate by independently contacting the supposed source utilizing an email address or telephone number that you know is valid.

Be especially suspicious of emails or websites that have typos or glaring errors.

NORTH Dakota | Financial Institutions
Be Legendary.™