Examples of Common Email Scams

Most email scams end up involving requests to send money, cash checks, establish business relationships or requests for information.

Nigerian Letter
This scam has been used for decades and has migrated from mail to faxes to email. An email will often start off with an introduction indicating that a government official (or some other person that would appear to have access to large amounts of funds) has died and left a large amount of money that is available to be transferred. The message then encourages the recipient to participate in the transfer in return for a share of the funds. Over time, the sender may ask for funds to cover taxes, bribes to others and legal fees that will be reimbursed once the funds are transferred.

Over the years, the deceased individual has been described as a minister of mining or natural resources, successful business owners and royalty. The locations have also changed over time.

There is no deceased official and no funds available to be transferred. The scam appeals to an individual's greed and a willingness to skirt foreign laws.

Canadian, South African, Netherlands, United Kingdom, "You Name It" Lottery
This scam appeals to one's greed and sense of being lucky. An email will arrive notifying the recipient that they have won a lottery. The email may even mention a legitimate lottery organization, but just because the email includes that name, the email is not from the organization. There is usually a request to keep the winning secret. The email then asks that a claims agent (or some other official sounding person) be contacted to arrange for payment. Once those conversations start, there is usually a request for funds to cover taxes, legal fees or other processing costs.

There are several things that should make one very suspicious:

- Unless you bought a lottery ticket, you are not going to win.
- Any taxes on lottery winnings are withheld from the payments and not paid up front.
- Legitimate lottery organizations do not charge fees.
- Most of these emails come from free email accounts like Yahoo, Hotmail, Gmail, MSN or those provided by an Internet service provider.

Check Cashing Schemes
These may take the form of an email indicating that the sender wants someone to cash checks in return for keeping a portion. "I will send a check made payable to you drawn on XYZ Bank in the amount of $10,000. All you have to do is deposit it. In return for doing this, you can keep $1,000 and wire $9,000 back to me."

This scam is usually promoted through emails but may also be found on job listing sites. The original check and the scam artist are usually from overseas, but not always.

The check may look real, but in reality, there is no account or the account has insufficient funds to cover the check. Because of the way check clearing works, funds are probably available to be transferred out before the incoming check has actually cleared. In this scam, the victim wires the $9,000 to the thief and a couple of days later receives word that the check he received has bounced. The result is a loss of $9,000.

Refund Scams

These schemes can take many forms, but usually involve an email indicating that the recipient has a refund due, but needs to provide information to speed the processing of the refund. The scam artists may claim to represent the IRS, state tax officials or even stores where someone may have purchased something.

The email directs the recipient to a website that may look legitimate but is a faked or spoofed site. Once there, the person will be requested to provide various personal information such as Social Security number, credit card number or account information so the refund can be directly deposited.

Providing this information is dangerous. Once in the hands of a fraudster, it can lead to credit card fraud, unauthorized access to your financial accounts or identity theft.

The IRS and most state taxing authorities do not use email to correspond about refunds. Commercial establishments may use email but you should be very wary of emails like this. Before providing the information online, contact the establishment by phone to make sure the request for information is legitimate.

Financial Account Confirmation Scams

Emails that request sensitive information are often called phishing emails. They often take the form of a message from a financial institution asking for the recipient to provide their account information due to a computer error, as part of a system upgrade or even as part of an enhanced Internet security initiative.

The recipient is usually directed to website that may look real, but is not. The information requested may include account numbers, user names, access codes and passwords. All of this information is dangerous in the hands of scam artists.

Financial institutions never ask for this type of information. If you receive this type of phishing email, contact your institution.

Article written by Financial Wisdom, advice is solely attributed to that entity.