GuidanceResources®

AVOIDING ONLINE FRAUD

Phishing is probably the most common type of online fraud. But with a little bit of information and common sense, it's also the easiest to spot.

Phishing is the act of sending an email message in an attempt to scam money from the recipient. People typically open these fraudulent messages because the email addresses appear to be from legitimate companies or even people they know.

Typically, these email messages contain a fake story or request designed to lure readers into clicking a link or button contained in the email. This link usually connects to an equally bogus website. There, the user is asked to surrender personal information such as passwords and credit card or bank account numbers. This information is usually used for identity theft.

Some phrases common to many phishing email messages include:

- Dear Valued Customer
- Verify your account
- If you don't respond within 48 hours, your account will be closed
- Click the link below to gain access to your account

Reputable banks, credit card companies and other institutions will never ask customers for the following information in an email message:

- Full name
- Password
- Credit and debit card numbers
- Pin numbers
- Bank account numbers

If you receive a phishing email message, you can protect yourself and your personal information in the following ways:

- Do not click on any link in the message or reply to the email.
- Do not call the phone number listed within the email.
- Do not download any attachment from the email.
- If the message mentions a legitimate company or institution, seek a phone or email listing for that company independently and report the phishing email.

Here when you need us.

Call: 888-972-4732
TDD: 800.697.0353
Online: guidanceresources.com
App: GuidanceResources® Now
Web ID: STATENV