Common Forms of Identity Theft
– Accessible Version

Phishing, pharming, and skimming are common forms of identity theft that you should be aware of.

Never provide bank, credit card, or other sensitive information when visiting a website that doesn't explain how your personal information would be protected, including its use of "encryption" to safely transmit and store data.

Be on guard against incoming e-mails claiming to be from a trusted source—perhaps a bank, another company you know, or even a government agency—asking you to "update" or "confirm" personal information. Reputable organizations won't contact you to verify account information online because they already have it.

**Phishing**
Phishing is when criminals send out unsolicited emails that appear to be from a legitimate source such as your bank, utility company, well-known merchants, your Internet service provider, or even a trusted government agency like the FDIC. Phishing emails attempt to trick you into divulging personal information.

**Pharming**
Pharming is similar to email phishing. Criminals seek to obtain personal or private information by making fake websites appear legitimate. In some cases, your browser will even show that you are at the correct website. This makes pharming more difficult to detect than phishing.

**Skimming**
Skimming is when criminals steal credit or debit card numbers by using a special storage device when processing your card. Watch for odd devices attached over the card slots of ATM machines for "skimming" or gathering information from the magnetic strip on the back of the card.