get home, carefully check them against your monthly statements.

In case your card is lost or stolen

Immediately contact your bank if your card gets lost, stolen, retained by an ATM, or you suspect that someone might have obtained your PIN.

Destroy expired cards by cutting them up.

Destroy cards that you are no longer using and inform your bank

DID YOU KNOW HOW TO PROTECT YOUR CARDS? PHISHING

What is phishing?

Phishing refers to online scams that attempt to trick consumers into revealing personal information, such as check and credit card account numbers, driver's license or bank account passwords.

Most commonly, phishers target unsuspecting users with fake Internet sites or email messages that look startlingly similar to the real thing. This is sometimes referred to as "spoofing." Scammers may also leverage social networking sites, where users are already accustomed to sharing information with others.

How does phishing work?

Phishing emails and websites typically use familiar logos and graphics to deceive consumers into thinking the sender or website owner is a government agency, bank, retailer or other company they know or do business with. Sophisticated phishers may include misleading details, such as using the company CEO's name in the email "from" field. Another common phishing tactic is to make a link in an email (and the fake website where it leads) appear legitimate by subtly misspelling URLs or changing the ".com" to ".biz" or another easily overlooked substitution.

Some phishing scams even lure victims by telling them that their information has already been jeopardized. For example, potential victims may receive an email that appears to come from a major bank warning that their account has recently been exposed to fraudulent activity. Users are asked to click a link within the message so they can "confirm" their bank account information. Instead of going to the bank's legitimate website, however, victims are taken to a clever lookalike, where their information actually is routed to identity thieves.

If you receive any message asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it's most likely a form of phishing. In addition to seeking bank information, phishers may also try to obtain your ATM PIN or any other bits of data that can help them build a more complete profile from which they can operate in your name.

Tips to avoid phishing

Consider all email requests for personal information to be suspicious

Do not respond to such emails or enter information on questionable websites

Check the legitimacy of the inquiry by contacting the number on the back of your credit card

Report suspicious emails or websites to your financial institution

IDENTITY THEFT

What is identity theft?

Using everyday items such as your driver's license, a thief can assume your identity to open new bank accounts, establish new credit card accounts, write bad checks, obtain personal or car loans, or get cash advances – all in your name. They may even set up cell phone or utility services and run up bills, in addition to making charges on your existing account, obtaining employment or renting an apartment using your identity. Just one instance of identity theft can negatively impact your credit score and may create problems