HARRIS COUNTY, TEXAS
The Bay Area Observer
ON THE WEB
Serving The Communities Along Galveston Bay

La Porte Police urge residents to be cautious of internet thieves

12-08-2011

Since the advent of internet-based communication and shopping methods has become available, the features have served as ones which many Americans have enjoyed and frequently taken advantage of. With increased product selection, added convenience, and the ability to engage in discussions immediately at our fingertips, these technological advancements have certainly proven extremely time-saving and helpful on many occasions for those who have made use of the services. However, there lurks an unseen criminal element who utilizes many available resources to commit serious acts of theft against unsuspecting consumers. The La Porte Police Department asks that residents take a moment to look over the following list of reminders published by the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center. Some of the current threat trends include, but are not limited to:

- Phony profiles on social networking sites such as Facebook and Twitter claiming to be legitimate businesses - Such fake profiles will look like their legitimate counterparts but clicking on links in these profiles could allow malicious code to be installed on the victim's computer compromising the victim's security and privacy.

- Hotel email's claiming that a "wrong transaction" has been charged to a credit card - The hotel will claim to offer a refund if the victim downloads and completes a refund form. Unfortunately, the form is embedded with malicious code and downloading it installs malware onto the victim's computer.

- Emails which are actually phishing scams involving bogus courier services during the holidays - The fake courier will send an email saying there is a package waiting for the victim and ask for personal information in order to retrieve it.

- Non-legitimate websites claiming to have the "hot" gift of the season while retailers are sold out - The non-legitimate websites will tempt the victim to order from them when they actually do not have the item and will steal their personal information and charge their credit card.

The following preventative strategies are intended to help citizens proactively look for emails attempting to deceive users into 'clicking the link' or opening attachments to seemingly real websites regarding holidays season 'deals'. The following are a few suggestions are offered by DHS and La Porte Police:

- NEVER click on links in emails

  If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.

- NEVER open the attachments

  Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.

- Do NOT give out personal information over the phone or in an email unless completely sure