Officials with the Indiana State Police Post in Sellersburg recently released information regarding a new scam being pulled on residents in the midwest.

? Identify thieves and online scammers attempt to obtain personal or financial account information from potential victims by “phishing.” Online scammers attempt to trick the potential victim into revealing personal information such as check and credit card account numbers, social security numbers, or bank account passwords. Typically “phishing” e-mails will lead the victim to what appears to be a legitimate website by informing them their bank account has been compromised or there are other problems with their account. They are directed to click on a link posted in the

e-mail. Instead of going to the bank’s official website, this link takes the victim to a fraudulent site that looks “official” where the victim will then be prompted to confirm personal or account information

“Smishing” is a form of “phishing” vis SMS (Short Message Service). With “smishing” the scammer will send the potential victim a text message on their cell phone posing as a financial institution and direct them to a fraudulent website or direct them to call a toll free number where they will again try to obtain personal or account information.

The tips below will help you avoid becoming a victim of identity theft through “phishing” or “smishing”:

Never provide personal or financial information over the phone or Internet if you did not initiate the contact.

If you get an e-mail or text message warning you that an account will be shut down unless you confirm information, do not reply or do not click on the link in the e-mail and do not use phone numbers given in the e-mail or text message. Contact the company requesting information via its public telephone listing.

If you get a phone call asking you to verify information for any reason, hang up immediately. Legitimate financial institutions will never do this.

Do not be intimidated by an e-mail, text message, or phone call that suggests dire consequences if you do not immediately provide or verify financial information. Again, legitimate financial institutions will never do this.

Avoid e-mailing personal or financial information. Before submitting financial information through a web site, look for the “lock” icon on the browser’s status bar. If you do not see one, do not submit the information.

Review credit card and financial statements as soon as they arrive to see if there are any unauthorized charges.

If you suspect you are a victim, act immediately and alert your financial institution. Place fraud alerts on your credit card accounts, monitor your credit report and account statements closely.

Report suspicious e-mails, text messages, or phone calls to the Federal Trade Commission at www.ftc.gov ro by calling 1-877-IDTHEFT.

For more information on how to protect yourself from identity theft or how to respond if you suspect you are a victim, visit the Federal Trade Commission’s “Fighting Back Against Identity

Theft” page at http://www.ftc.gov/bcp/edu/microsites/idtheft/.