

Online Security

Different Types of Fraud



German American State Bank is dedicated to protecting you and your finances from fraud but we need your help. Keep a look out for the different types of online fraud listed below to avoid becoming a victim of identity theft.

Phishing

Phishing is a scam involving fraudsters who present themselves as a legitimate business in an effort to trick you into divulging your personal information. They contact you via email and pretend to be a reputable business (ex: bank, credit card company, online provider) in immediate need of your personal information to update their records or prevent a disruption in service.

Vishing

Vishing (or VoIP phishing) is when fraudsters use the telephone to attempt to gain your personal information. They will call you from a fraudulent phone number or email you stating to call a number for some urgent need. Once they gain your trust they convince you to provide them with your personal information.

Smishing

Smishing uses cell phone text messaging to lure consumers into giving out their personal information. A consumer typically receives an urgent text with a link or phone number to call. Like the other phishing scams they then convince you to give out your personal information for various reasons.

Pharming

Pharming is a type of Phishing where the fraudster acquires access to your computer to install a malicious code. This code redirects you to a fraudulent website, without your consent or knowledge. The fraudster seeks to obtain your personal account information such as PIN and account numbers.

Malware

Malware, short for malicious software, is software used to access your computer without your knowledge. Malware can be downloaded on your device simply by clicking on a banner ad or fraudulent document.

Remember GASB will never call or e-mail you to verify account information. If you suspect you have been a victim of identity theft notify us immediately by calling (815) 362-2310.

For more information visit:

www.germanamericanstatebank.com/resources/fraud-center.html

German
American
State Bank

Member FDIC

Online Security

Continued



Remember GASB will never call or e-mail you to verify account information. If you suspect you have been a victim of identity theft notify us immediately by calling (815) 362-2310.

Tips for Preventing Identity Theft

- Do not respond to unsolicited e-mails, telephone calls, or text messages that ask for personal information. Never click on unsolicited emails; instead always type in a web address you know.
- Use firewalls, anti-spyware, and anti-virus software to protect your computer, tablet, mobile phone or other device. Install updates to the software as needed.
- When creating passwords or passcodes, avoid using obvious numerical sequences (for example:1234), your birth date, your Social Security number, or your mother's maiden name. Create passwords for your mobile device so it can't be used if lost or stolen.
- Trust your instinct. If something doesn't appear right, do not provide information and report the event to local police, bank or other potentially impacted party.
- Do not give out any personal information to anyone calling you. German American State Bank will never call you asking for your card number, personal PIN or account number(s). Please contact the bank at 815.362.2310 immediately if you receive such a call requesting this information.

For more information on how to avoid becoming a victim of identity theft and what to do if you if you have fallen victim visit:

www.germanamericanstatebank.com/resources/fraud-center.html

