KCSB

KALAMAZOO COUNTY STATE BANK

YOUR JOURNEY. YOUR BANK.

SCHOOLCRAFT • MICHIGAN 49087 • TELEPHONE (269) 679-5291
MATTAWAN • MICHIGAN 49071 • TELEPHONE (269) 668-3386
VICKSBURG • MICHIGAN 49097 • (269) 649-0001

Beware of Phishing – Tips to help spot the phish

Phishing is a fraudulent attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source. The phishing email might ask you to collect personal data such as login credentials, credit card numbers, social security and bank account numbers, or prompt you to open a malicious attachment that infects your computer with a virus or malware.

Be Vigilant – Vigilance is Key

How do you tell the difference between a phishing message and a legitimate message? There is no single technique that works in every situation.

Be aware of these attempts:

1. Don't trust the display name. Always check the sender's email address. When a hacker sends fake emails, they opt to obscure the sent address with a name that might be familiar, like 'John Smith'. Be sure to check the originating email address and determine if it's genuine.

2. Reply-to address is not the same as the sending address. If the reply-to address is different than the sender's address, this should raise suspicion.

3. Look but don't click. Hover your mouse over any links found in the email. Dangerous links are masked as safe links. If the link looks weird, don't click on it.

4. Check the message for poor spelling and grammar. Legitimate messages usually do not have major spelling/grammar mistakes.

5. The message asks for personal information. Most companies will not request confidential information via email.

6. The offer seems too good to be true. If you are promised money or prizes, use extreme caution. Don't believe everything you see.

7. Review the signature. Lack of details about the signer could suggest a phish. Legitimate businesses always provide contact details.

8. The message invokes a sense of urgency. Fraudsters often include urgent “calls to action” to try to get you to react immediately. Be wary of emails containing phrases like “your account will be closed”.

9. Don’t open attachments you weren’t expecting. Malicious attachments could contain malware.

10. Something just doesn’t look right. Always be skeptical when it comes to email messages.

Phishing is not to be confused with Spam – a form of junk mail. Spam is an irrelevant commercial, an unsolicited email, typically sent in bulk. Phishing emails attempt to convince users to surrender information through a variety of tactics including email attachments, familiar links, and other suspicious requests prompting you to transfer funds, or provide sensitive information.

Member FDIC