Farmers & Merchants Union Bank
fmub.bank

There is an estimated 3.4 billion phishing emails sent each day by cybercriminals - many of these emails target businesses. Now you could have access to $100,000 Cyber Liability Policy and dark web monitoring for mentions of your organization's domain thanks to FMUB's partnership with Cyber Protect Identity Watch from Fiserv.

IDENTITY THEFT PROTECTION
that helps you connect with confidence

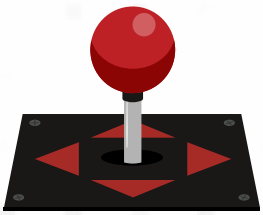
To learn more and to enroll now, visit fmub.bank/ID-Watch.aspx or call one of our friendly and knowledgeable bankers at 920.623.4000.

fiserv. CyberProtect℠ Identity Watch

Insurance products are sold by Chubb Limited and its licensed agents.
Insurance products are: Not FDIC insured | No Bank Guarantee | May Lose Value | Not a Deposit
Not Insured by any Federal Government Agency

Member FDIC

Farmers & Merchants Union Bank
fmub.bank



Recognizing and reporting phishing

Cybercriminals sent over 3.3 billion phishing messages and caused over 4,000 data breaches, exposing over 22 billion personal records. But it isn't enough to simply know that phishing emails are out there; you also need to be able to recognize and report them in order to protect your business, which is why your friends at Farmers & Merchants Union Bank are sharing these tips on how to spot a phishing email with you.

Look at some of the highly used phishing email types and tactics

Reward or free gift message

Free things are enticing, but they can also be dangerous. If you get an email saying you won a free TV or "click here to enter a prize drawing," be on high alert! Ask yourself if a message like this would come to your work email; if not, its probably a scam. Hackers are trying to bait you into clicking a malicious link.

Login or password message

Another type of phishing email asks you to verify your account by logging into a (fake) webpage or updating your credentials. These emails can collect your username and password, giving a hacker instant access to your account. If this is a vendor you are familiar with, ask yourself if this aligns with their normal business activity? If not, its more than likely a scam.

Urgent message

An urgent phishing email is designed to get you to act fast without thinking. It might tell you that your account was compromised and to fix it before anyone at your company finds out, click here to restore it! Fear makes people do things without thinking, so slow down!

Internal messages

Hackers will try to impersonate people at your company, such as someone in the HR or IT department. An internal message phishing email might ask you to click on a link to read and sign a policy, read a document about a company-wide update or even hand over sensitive information. The best way to combat this type of fraud is to contact the coworker who 'sent' you the message and verify it was indeed them who sent it.

If you think you may have encountered a phishing email, follow your company's procedures for reporting. Once the right people are notified, they can help you determine if it's a phishing email. Whatever you do, do not click on any links, reply to the email or send it to anyone else!

And remember, anytime you think you or someone at your company may have encountered a phishing email, be sure to call the friendly and knowledgeable bankers at Farmers & Merchants Union Bank. Chances are, we've seen the scam already and can help you navigate it in a professional and confidential manner.

Information from our friends at
INFOSEC

©2022 Infosec, Inc. All rights reserved.