Since 1887

FARMERS
NATIONAL BANK

# Fraud, Cybersecurity and Small Business

# HOW CAN I PROTECT MY BUSINESS?

## Train Your Employees

- Your best defense is an informed workforce. Explain to your staff how scams happen.
- Encourage people to talk with their co-workers if they spot a scam. Scammers often target multiple people in an organization.
- Train employees not to send passwords or sensitive information by email, even if the email seems to come from a manager.

## Know Who You're Dealing With

- Before doing business with a new company, search the company's name online with the term "scam" or "complaint." Read what others are saying about that company.
- When it comes to products and services for your business, ask for recommendations from other business owners in your community. Positive word-of-mouth from trustworthy people is more reliable than any sales pitch.

## Be Tech-Savvy

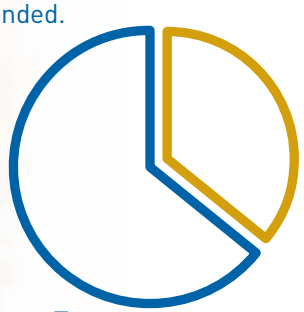
- Imposters often fake caller ID information so you'll be more likely to believe them when they claim to be a government agency or a vendor you trust.
- Remember that email addresses and websites that look legitimate are easy for scammers to fake.
- Secure your organization's files, passwords and financial information.

## Verify Invoices and Payments

- Never pay invoices unless you know the bill is for items that were actually ordered and delivered.
- Make sure procedures are clear for approving invoices or expenditures. Limit the number of people who are authorized to place orders and pay invoices.
- Pay attention to how someone asks you to pay. If you are asked to pay with a wire transfer, reloadable card, or gift card, you can bet it's a scam.

## Vigilant Security Practices

- Keep anti-virus software up to date and run scans at least weekly.
- Download Trusteer, a free malware and fraud protection software that Farmers offers to its customers.
- Maintain complex passwords on all computer systems and applications including email accounts. Passwords should be at least 10 characters long and use a combination of upper and lower case letters, numbers, and special characters(i.e. !, *, #, etc.).
- Use a separate bank account for incoming wire transfers or utilize an online wire payment service in order to minimize the possibility of account compromise.
- Educate your employees regarding phishing scams and instruct them to not click on email links or provide any personal or financial information to unknown individuals.
- Keep checks in a secured area and only allow access to authorized individuals.
- Review your bank account activity frequently - daily is recommended.



***The average cost of lost business for organizations in the 2019 study was $1.42 million,***

***which represents 36 percent of the total average cost of $3.92 million.****

**According to the 2019 IBM Security Cost of Data Breach Report.*

# INFORMATION AND ACCOUNT SECURITY

## Ongoing Fraud Deterrence Efforts

- Outgoing wire call back procedures
- Annual vulnerability assessments and training
- Internal cyber threat exercise to determine top cyber threats to banks and remediation
- Credit and debit card fraud monitoring
- Real-time verification telephone calls to cardholders for suspect transactions
- Annual information security risk assessment
- Rigorous vetting process for third-party business partners

## Products/Services

- Check Positive Pay
- ACH Positive Pay
  Debit blocker | ACH filter | ACH Positive Pay
- Trusteer Rapport
- Multi-factor authentication and out of wallet
- Security token
- Required password complexity

## Password Security

Because your online and mobile banking passwords are used to access your accounts, you should treat them as you would any other sensitive personal data. You should:

- Carefully select a password that is hard to guess and keep it safe.
- Do not disclose your password by telephone or to anyone claiming to represent Farmers National Bank.
- Notify Farmers National Bank immediately if you suspect that an unauthorized person has access to your password or believe your password has been lost or stolen.

## Online and Mobile Banking Security

Mobile banking provides the convenience of online banking to you on the go. However, your mobile device can also be impacted by the same attacks as a desktop computer. Here are some helpful tips to help keep you safe:

- Only install the official banking application from the Apple Store or Google Play Store.
- Don't open suspicious email or attachments on your mobile device.
- Use caution when visiting an unknown site.
- Consider installing antivirus software for your mobile device.

# Farmers is serious about protecting your business.

We continue to invest in advanced technology and implement evolving security procedures to make your banking more secure.

**Please contact our Treasury Management Team at**
330.505.3944 or treasurymanagement@farmersbankgroup.com
for additional information or assistance.

since 1887
FARMERS
NATIONAL BANK

1.888.988.3276
farmersbankgroup.com

Follow us on:

Equal Housing LENDER
MEMBER FDIC