Business Email Compromise

How we protect your business.

OLD NATIONAL®
Your bank. For life.™

We take information security seriously. Before discussing sensitive matters or performing a transaction, we request valid identification at our banking centers or use authentication questions when you call us. Old National will never request you provide information such as your account number, card number or social security number via email or text. To protect you, we do not perform transactions or account maintenance or provide sensitive information via email or text. If you email us, we will confirm with you through another channel.

What to do if you receive a suspicious email or provided sensitive information?

- Confirm ANY ***email request for payment, change in payment instructions*** or sensitive information directly with the sender-even email from within your own company.
- Confirm with the sender through a channel other than email such a known phone number (not one provided in the email).
- If you have shared your card number, call the number on the back of the card and report your number as potentially compromised.
- If you have shared other sensitive information (account number, social security number, etc) via an email (or text) and believe your information may be in jeopardy, contact your Old National Representative or Old National Client Care by calling 1-800-731-2265. Depending upon the specific circumstances, you may also need to file reports with the local police, FTC, IC3 and the three major credit bureaus.

Steps you can take to protect your business.

- Use different, unique, complex passwords for each account and change passwords periodically.
- Do not post personal information that might be used for password resets on social media.
- Be aware or similar but not exact email addresses (johnsmiih@gmail.com vs. johnsmith@gmail.com)
- Never provide sensitive information (account number, social security number, card number, date of birth, mother's maiden name) via email or text.