

Phishing

Most likely you've seen them: email messages asking you to verify personal information over the Internet.

The scam, popularly called 'phishing,' involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial or password data. Often suspects use urgency or scare tactics, such as threats to close accounts.

We here at Illinois National Bank will never ask you via email to verify account information. We will never use email to threaten account closure. Please know this, as this is your number one defense against phishing. Other safeguards to help protect you from phishing scams:

- Be suspicious of any email messages that claims to be from us that use an urgent or scare-tactic tone.
- Do not respond to email messages asking you to verify personal information.
- Delete suspicious email messages without opening them. If you do open a suspicious email message, do not open any attachments or click any links.
- Install and regularly update virus protection software.
- Keep your computer operating system and Web browser current.

If you see a suspicious-looking email message claiming to be from Illinois National Bank, please let us know by email at abuse@illinoisnationalbank.com or you may also contact our customer service department by email at customerservice@illinoisnationalbank.com or by phone at 217-747-8766. We continually monitor such reports and act on them promptly. Additionally, also consider contacting the FBI's Internet Fraud Complaint Center at www.ifccfbi.gov.