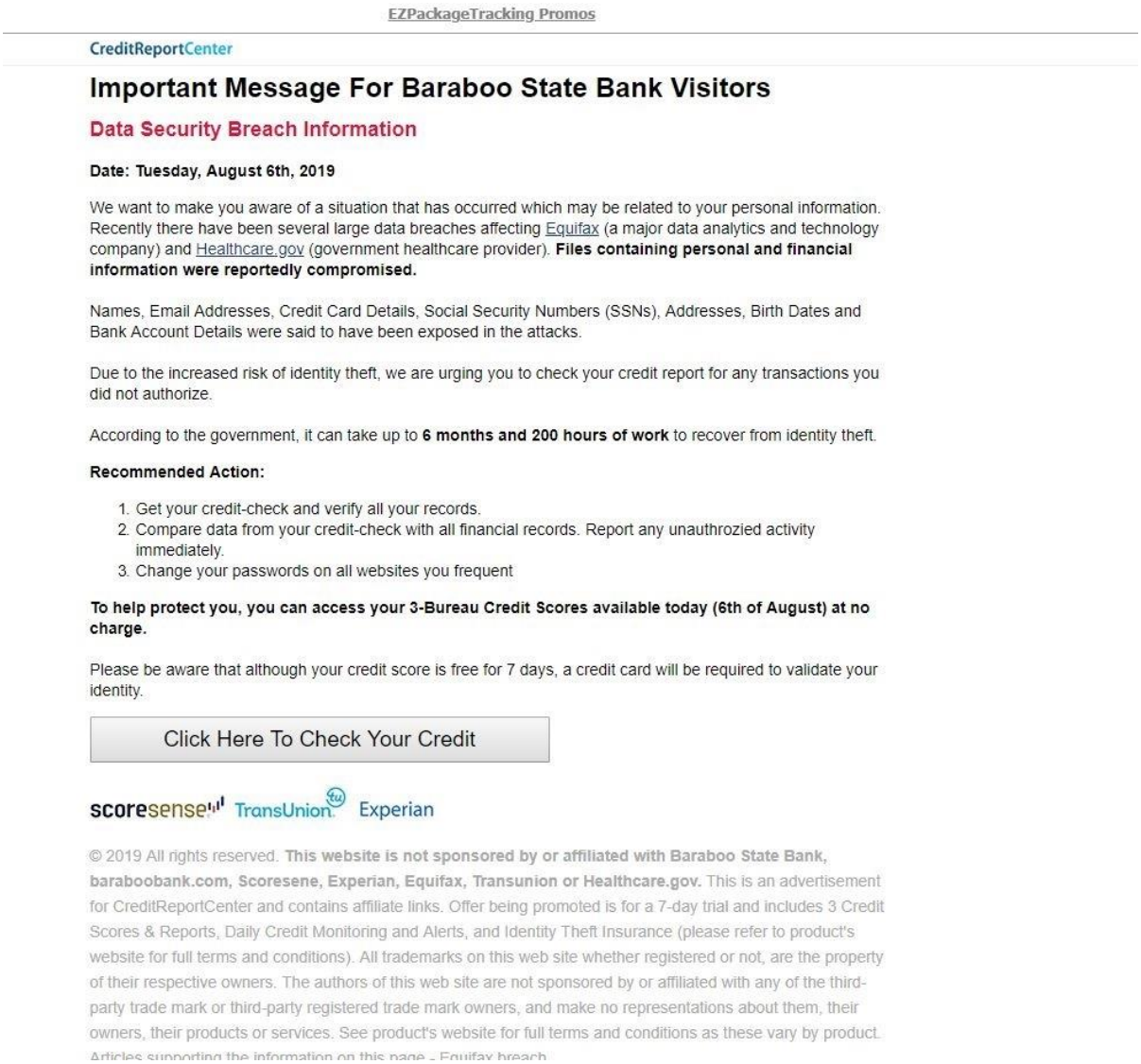
Most recent sample of a phishing scam below



EZPackageTracking Promos

CreditReportCenter

Important Message For Baraboo State Bank Visitors

Data Security Breach Information

Date: Tuesday, August 6th, 2019

We want to make you aware of a situation that has occurred which may be related to your personal information. Recently there have been several large data breaches affecting Equifax (a major data analytics and technology company) and Healthcare.gov (government healthcare provider). **Files containing personal and financial information were reportedly compromised.**

Names, Email Addresses, Credit Card Details, Social Security Numbers (SSNs), Addresses, Birth Dates and Bank Account Details were said to have been exposed in the attacks.

Due to the increased risk of identity theft, we are urging you to check your credit report for any transactions you did not authorize.

According to the government, it can take up to **6 months and 200 hours of work** to recover from identity theft.

Recommended Action:

1. Get your credit-check and verify all your records.
2. Compare data from your credit-check with all financial records. Report any unauthrozied activity immediately.
3. Change your passwords on all websites you frequent

To help protect you, you can access your 3-Bureau Credit Scores available today (6th of August) at no charge.

Please be aware that although your credit score is free for 7 days, a credit card will be required to validate your identity.

Click Here To Check Your Credit

scoresense TransUnion Experian

Articles supporting the information on this page - Equifax breach

Phishing: Don’t Take the Bait

Phishing is when you get emails, texts, or calls that seem to be from companies or people you know, but they’re actually from scammers. They want you to click on a link or share personal information (like a password or social security number) so that they can use that information to steal your money and/or identity.

The Bait

- Scammers use familiar company names or pretend to be someone you know. They send a text or ‘spoofed’ email or even call you in a way that makes it appear to be from a friend, family member, or an employee of a trusted organization like your bank, Credit Card Company, government agency or Phone Company.
- The bait may look and sound like a legitimate request. The scammers might even have personal information about you, like your date of birth or password.
- They often say they need your information now, to protect your account, to help a loved one in trouble, or to confirm login or password information and warn that something bad will happen if you do not act immediately.
- They ask you to give sensitive information like passwords or bank account numbers or they ask you to click on a link. If you click on the link, they can install malicious programs that can lock you out of your computer or enable them to gain access to use your personal or financial information, even from outside of the country.

Avoid the Hook

- Take a few minutes to check a request out. You wouldn’t give your house keys to someone you don’t know or trust. Don’t give someone the keys to your bank account before you know who that person is and are certain that person can be trusted.
- If someone calls asking for information or wants you to act, tell the caller you will call back, then call the number on your billing statement or credit card to report the call. If the caller tries to convince you to stay on the phone, it’s a scam. Hang-up and call the trusted number.
- If it’s an email, don’t click on it. Go to the company’s website using a bookmark or type it in and check for alerts on your account.
- If you’re unsure, ask a friend, coworker, family member, or caregiver to help.

Look for Scam Tip-Offs

- You don’t have an account with the company.
- The email, text or caller is asking for account information, including passwords.
- Grammatical errors or something just seems fishy or not right.

Protect Yourself

- Keep your computer and mobile device security software up to date and regularly back up your data.
- Change your security settings to enable multi-factor authentication—a second step to verify who you are, like a text with a code—for accounts that support it.
- Change any compromised passwords right away and do not reuse those passwords for other accounts.
- Use a cloud-based account such as Google Drive or Microsoft OneDrive that can allow you to restore your data if your computer is comprised.
- Don't provide any information to anyone who calls or emails you out of the blue. Only do it if you've called or emailed them.

Please do not hesitate to reach out to any of our representatives if something does not seem right.

608-356-7703 or stop into any of our locations for assistance.

BARABOO STATE BANK

banking better together