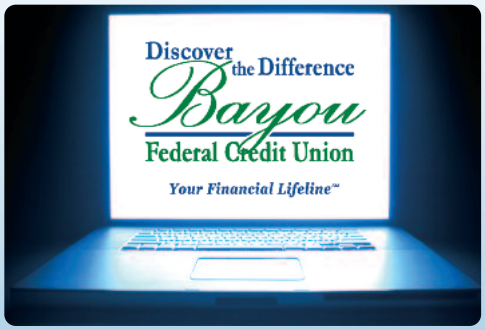
PHISHING ATTACKS
ALERT



Fraudsters posing as fraud team representatives to drain account funds

November 21, 2019

Financial institutions around the country are reporting phishing attacks on accountholders where criminals are posing as a fraud team representative from the institution.

These attacks have resulted in as much as $10,000 in losses from a single attack.

In these attacks, the fraudster calls, texts, or emails the accountholder to "verify" multiple pieces of private information so they can gain access to the account and drain it of funds. In many instances, criminals "spoof" the financial institution's phone number so it shows up as such on the accountholder's caller IDs. Information requested of the accountholder includes, but is not limited to:

- Online banking user name and password
- PIN number
- Security codes
- Account number
- Card number

Here is what you can do NOW to mitigate exposure to these crimes:

- Be aware that fraudsters are posing as fraud team members, and they can "spoof" our phone number to make it look as if the call is coming from Bayou Federal. They can also make texts and e-mails appear as if they're coming from Bayou Federal.

- Know that Bayou Federal does not call, text, or e-mail members to ask for personal information such as passwords or PIN numbers. If you receive such a request, call us directly to report the incident.

- Remain vigilant when using your accounts, cards, and any of our services. Fraudsters are working to learn your information so they can try to empty your accounts!

- Always keep your personal information private, and learn more about phishing and other methods of fraud by visiting ftc.gov.

Additional tips and information:

Scams

Be on the alert for credit scams or any related terms. You'll see these in emails, ads on social sites or games, and even physical mail to your home. These attacks are part of what we refer to as social engineering, and they will run rampant for many months and years to come. Always be skeptical, and if you're not sure about something, ask a professional.

Phone or text scams

Since your data was most likely taken, that means your numbers will be shared even more than they already are today. Calls and texts from unknown numbers, numbers with similar area codes, or numbers very similar to yours should be treated as potential scams. You might think that the National Do Not Call Registry would protect you from this. Sadly, it does not. It offers protection from legitimate companies trying to solicit your business. It does not offer protection against scammers. (Because why would criminals follow the law, anyway?)

My Social Security account

The my Social Security account allows you to keep track of the social security funds you'll be collecting in the future. Although it was not affected by the Equifax breach, it's good practice to get this account set up in your name, as someone else could easily grab it and you'd be locked out of your future payments. One caveat: If you want to set up this account, you'll need to do it before you freeze your credit. (Otherwise they can't confirm your identity through the account.)

Passwords and two-factor authentication

Ensure you're using smart password strategy (complex, do not repeat them, do not use the same one across multiple sites/services, etc.) and if available, enable two-factor authentication (2FA) on every account possible.

Enable alerts on your accounts

While your current accounts shouldn't be impacted by this breach, it's never a bad idea to keep an eye on your bank accounts and credit cards for larger purchases. For accounts rarely used, you could set alerts to $1 so you're notified the second any transaction happens. For regular accounts, set the alerts to a dollar amount that would seem out of place for that card, whether it's $20 or $500.

New phone accounts

A common attack vector with credit/personal data breaches is to purchase new phone accounts through your provider, with your account! Once criminals have your info, they'll call up the phone company and say they want to add a new line but don't have a PIN number. If you haven't set up a PIN number with your phone company already, they have no way to verify your account. So guess what? BAM! There's a new phone on your bill. In order to protect yourself from this type of attack, go ahead and set up a PIN with your provider.

Taxes

File these as soon as possible next year! For multiple years we've heard about victims of tax return fraud, wherein a scammer using your personal information files YOUR return before you can. So don't wait on this one.

Summary

Remember, one new credit card created by an attacker in your name is going to cause a massive headache. Better to stay ahead of it than spend the next month trying to convince a bank or credit union that you didn't open an account. Take some time now to protect yourself and your accounts. It will be worth it.

For More Information

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft