

You should not disclose your personal information over the phone or Internet.

What to do if you fall victim:

Contact your financial institution immediately and alert it to the situation.

If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:

Equifax
800-525-6285
P.O. Box 740250
Atlanta, GA 30374

Experian
888-397-3742
P.O. Box 1017
Allen, TX 75013

TransUnion
800-680-7289
P.O. Box 6790
Fullerton, CA 92634

Report all suspicious contacts to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

How to protect yourself:

Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone, or the Internet if you did not initiate the contact.

Never click on the link provided in an e-mail you believe is suspicious. It may contain a virus that can contaminate your computer.

Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.

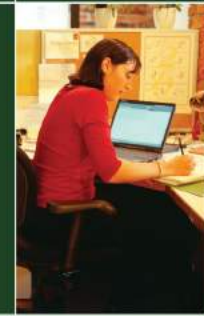
If you believe the contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously bookmarked, instead of a link provided in the e-mail.

If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.

Report suspicious e-mails or call to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.



Member
FDIC



Prevent Identity Theft

You can prevent identity theft. Badger Bank works with you to protect your privacy.

 **Badger Bank**

Badger Bank works with you to protect your identity and ensure your financial safety at all times.

How phishing works:

In a typical case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required", or "Please contact us immediately about your account". The e-mail will then encourage you to click on a button to go to the institution's website.

In a phishing scam, you could be redirected to a phony website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth. **If you provide the requested information, you may find yourself a victim of identity theft.**

A type of Internet piracy is called "phishing". It's pronounced "fishing", and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

How to protect yourself:

1. Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.

2. If you believe the contact may be legitimate, contact the financial institution yourself. You can find phone numbers and websites on the monthly statements you receive from your institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified.

Quick Tip: If you feel you are a victim of a phishing scam or are aware someone is phishing for your information, contact Badger Bank immediately.



3. Never provide your password over the phone or in response to an unsolicited Internet request. A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.

4. Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.

 **Badger Bank**