

What is phishing?

Phishing is a new type of identity theft that occurs online. Scam artists steal personal information from consumers by creating fraudulent Internet pages. The damage inflicted by these “phishers” can hurt your reputation and damage your credit rating for years to come.

How phishing occurs

Phishers send emails that appear to come from reputable sources, such as financial institutions or credit card companies. Some emails appear to come from the federal government or another regulatory agency.

These emails typically warn that you need to update your information or request that you take immediate action regarding one of your accounts. They tell you to click on an icon or link to be directed to the institution’s website.

Here is where the scam comes in. When you click on the link or icon, you are directed to a phony webpage that looks very similar to the actual site for that institution, often incorporating identical logos and hyperlinks. Or you are directed to the real website and a pop-up window quickly appears in front of the home page. This window is created by the scam artists.

The webpage or pop-up window directs you to type in personal information, such as your account number, password or Social Security number. If you provide this information, it goes directly to the crooks—not to the company with whom you transact business. Then they are able to access your accounts.

Don't be the catch of the day

Here are a few tips to prevent becoming a victim of phishing:

1. **Never respond to unsolicited requests for personal information.** Financial institutions and credit card companies will not ask you to verify this information by phone or online.
2. **Contact the company yourself** if the message appears to be from a company you deal with. Close the email and log on to your account directly or call using contact information that you know to be accurate. Do not use the information provided in the email.
3. **Review all financial statements closely** to ensure all transactions displayed were actually made by you.
4. **Request your credit report** from the three credit bureaus at least once a year and review the accounts and payment histories closely.



What to do if you're a victim

If you think you've been a victim of a phishing scam, here are the steps you should take:

1. **Contact your financial institution** and let them know that your account information may have been compromised.
2. **Contact the three major credit bureaus** and request that a fraud alert be placed on your credit file. This will prevent Internet thieves from opening new accounts in your name.

Major Credit Bureaus:

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

Experian (888) 3973
P.O. Box 1017
Allen, TX 75013

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

3. **Report all phishing activity** to the Federal Trade Commission at www.consumer.gov/idtheft or call (877) IDTHEFT.

Is someone
"phishing"
for your
personal
information?

Don't be the
catch of
the day.