You Have the Power to Stop Identity Theft

Stop Identity Theft

There is a type of identity theft using the Internet called “phishing.” Pronounced “fishing,” that’s exactly what thieves are doing, fishing for your personal financial information. They want your account numbers, passwords, Social Security numbers, and other confidential information so they can use your financial accounts or run up bills on your credit cards.

In the worst case, you could find yourself a victim of identity theft. With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even a driver’s license in your name. **They can do damage to your financial history and personal reputation that can take years to unravel**. But if you understand how phishing works and how to protect yourself, you can help stop this crime.

How phishing works

Typically, you’ll receive a phone call or an e-mail that appears to come from a reputable company you recognize and may do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, perhaps a federal financial institution regulatory agency.

A. **Phone phishing:** The call usually begins with an urgent fraud warning on your account and asks you to immediately verify your entire debit card number or account number, as well as personal information such as the three digit code on the back of the card and sometimes you PIN. The phishers typically use and automated system and prompt you to enter your information.

B. **E-mail phishing** usually warns 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 may also state that unless you provide certain confidential information your account will be deactivated or closed. The e-mail will encourage you to click a link to go to the institution’s Website.

Phishing scams may also occur through Website redirection to a phony Website that may look exactly like the real site. 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 collecting your financial information. 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 your 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.**

How to protect yourself

1. **Never provide your personal information in response to an unsolicited request,** whether it is over the phone or on 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, ***do not*** **provide** any information.
2. **If you are unsure whether a contact is legitimate, contact the financial institution.** You can find phone numbers and Websites on the monthly statements you receive from your financial institution, or you can look up the company in a phone book or on the Internet. The key is that ***you*** should be the one to initiate the contact, using information that you have verified yourself.
3. **Never provide your account information and/or password over the phone or in response to an unsolicited Internet request.**

A financial institution would never ask you to verify your account information or confirm a password online. Thieves armed with this information and your account number can help themselves to your money.

4. **Review account statements regularly to ensure all charges are correct.** If your account statement is late in arriving or does not arrive, call the bank to find out why. Sign up for Online Banking and check your account activity online regularly to catch suspicious activity.

What to do if you fall victim

- Contact Colonial Federal Savings Bank immediately to place an alert on your accounts. **Phone: 617-471-0750**

- Close accounts you think have been tampered with or opened fraudulently. Call the security or fraud department of each associated company or financial institution. Follow-up in writing with copies of supporting documents.

- It is important to notify credit card companies and financial institutions in writing. Send your letters by certified mail, return receipt requested, so you can document when and what the company received. Keep copies of your correspondence and enclosures.

- Report all suspicious contacts to the Federal Trade Commission through the Internet at ftc.gov/bcp/edu/microsites/idtheft/, or by calling **1-877-IDTHEFT (1-877-438-4338)**.

- File a report with local police or police in the community where the identity theft took place. Obtain a copy of the police report or the report number. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report.

If you disclose sensitive information in a phishing attack, contact one of the three major credit bureaus listed below and discuss whether to place a fraud alert on your file. A fraud alert will help prevent thieves from opening a new account in your name.

Equifax:	**800-525-6285**	P.O. Box 740250, Atlanta, GA 30374	equifax.com
Experian	**888-397-3742**	P.O. Box 1017, Allen, TX 75013	experian.com
TransUnion	**800-680-7289**	P.O. Box 6790, Fullerton, CA 92634	transunion.com

You can fight identity theft - Here's how:

- **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 think is fraudulent.** In addition to stealing your personal information, the link 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 are unsure whether a contact is legitimate, go to the company's Website** by typing in the site address or using a page you have previously book marked, instead of using a link provided by the e-mail.
- **If you fall victim to identity theft, 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 calls** to the Federal Trade Commission through the Internet at ftc.gov/bcp/edu/microsites/idtheft/, or by calling **1-877-IDTHEFT (1-877-438-4338)**.

To learn more about keeping your money safe, visit mymoney.gov

---

Member FDIC

EQUAL HOUSING LENDER

COLONIAL FEDERAL SAVINGS BANK