

ACTION

What to Do If You Become a Phishing Victim

Forward Phishing Emails to

- Federal Trade Commission (FTC) at spam@uce.gov – and to the company, bank, or organization impersonated in the email.
- United States Computer Emergency Readiness Team at phishing-report@us-cert.gov
- You may also report phishing email to the Anti-Phishing Working Group (APWG) at reportphishing@apwg.org

If you might have been tricked by a phishing email:

- File a report with the Federal Trade Commission at www.ftc.gov/complaint.
- Visit the FTC's Identity Theft website at www.ftc.gov/idtheft. Victims of phishing could become victims of identity theft.

Identity Theft Victim Action

1. Call FTC Identity Theft hotline (1-877-438-4338). Counselors will direct you to file a complaint and obtain the Federal Trade Commission's (FTC) booklet, "Taking Charge – What to Do if Your Identity is Stolen" (www.ftc.gov/idtheft)
2. Place a fraud alert on your credit report, and review credit reports. A fraud alert can be placed by contacting **one** of the big three (3) credit reporting agencies online at www.annualcreditreport.com or by phone as listed below, (the company you contact is required to contact the other two companies) and:
 - ✓ Inform them that you are a victim & want to review your reports;
 - ✓ Request that a fraud alert be placed on your file; and
 - ✓ Include a statement requesting that you be contacted before any account change or new account is opened.

Equifax: 1-800-525-6285

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289
3. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.
4. File a police report.
5. Use police report to place free extended fraud alerts and obtain security freezes.

Keep written records of all your activities, and send all correspondence certified mail, return receipt requested, so you can document if and when the correspondence was received.