



What Should I Do If I Accidentally Released Information To A Phishing Site?

Question: I recently disclosed some personal information on a site that I believed was legitimate but now know was a phishing scam. What should I do to avoid becoming the victim of identity theft?

Answer: So sorry to hear of your predicament. You're not alone; phishers are getting increasingly sophisticated and manage to get many people to disclose information like credit card numbers online. Depending on what information has been compromised, here are some key steps to take:

- **Report the theft to the three major credit-reporting agencies** (Experian, Equifax, and TransUnion Corporation). Request that they place a fraud alert and a victim's statement in your file, and remove inquiries and/or fraudulent accounts stemming from the theft. You should also get a free copy of your credit report to check whether any accounts were opened without your consent.
- **Notify your bank(s)** and ask them to flag your account and contact you regarding any unusual activity.
- **Change the passwords** on all user ID accounts that you gave out. Make sure to tell the company that maintains your compromised user ID account that you have given your password to a phishing site, and make sure there hasn't been any irregular activity on your account(s).
- **Document the names and phone numbers of everyone you speak to regarding the incident.** Follow-up your phone calls with letters and keep copies of all correspondence.

For additional information to help you fight back against identity theft, visit: www.ftc.gov/bcp/edu/microsites/idtheft