

Brand Spoofing is a scam in which perpetrators disguise themselves as well-known companies and "phish" for personal information.

What are the identity thieves looking for?

- Social Security Numbers
- Date of Birth
- Passwords or PINS
- Account Numbers (credit card, bank)
- ATM / Debit Card Number

How is the crime attempted?

E-Mails are sent to people asking them to click onto a link (spooft web site). Disguising themselves as your company, they ask you to either provide, confirm, or update confidential information. The e-mails generally express a sense of urgency, importance, or threatening situation regarding your account. Even if you do not provide the requested information, the act of just clicking onto the link makes your computer susceptible to Trojan Horses (key logging software) or other viruses.

You may not do business with the company or financial institution used in the scam. The perpetrators send the e-mails to thousands of individuals hoping to hit on a person who has an account or does business with the named company.

Common subject headers used to attract your attention

- Security Update
- Proposed Account Suspension
- Please Confirm Your Account
- Fraud Check Verification
- Confirmation needed
- Dear Client of _____

Be on the lookout for

- Spelling errors in the e-mail
- Awkward sentence structure (sentence fragments)
- Links embedded in the message narrative that contain all, or part, of legitimate company's name

House Number:

The Haworth Police Department would like to remind all residents that house numbers should be very prominently displayed upon their homes. Haworth Borough ordinance requires that house number be clearly visible from the street. This enables responding emergency personnel to quickly provide emergency services to those in need. We thank you for your anticipated cooperation.