Pretexting is a form of social engineering in which one individual lies to obtain privileged data about another individual in order to engage in identity theft or corporate espionage. A pretext is a false motive.
Pretexting is a form of social engineering in which an individual lies to obtain privileged data. A pretext is a false motive.

Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person he is talking to. After establishing trust with the targeted individual, the pretexter might ask a series of questions designed to gather key individual identifiers such as confirmation of the individual's social security number, mother's maiden name, place or date of birth or account number.

Pretexting to gain access to financial data was specifically banned by the Gramm-Leach-Bliley Act (GLB) in 1999. The pretexting restrictions defined by GLB apply to all organizations that handle financial data, including banks, brokerages, credit unions, income tax preparers, debt collection agencies, real estate firms and credit reporting agencies. The Act's restrictions do not apply to information that enters the public domain as a matter of public record, such as details of real estate transactions, property taxes, bankruptcy or police records.

The distinction between legal and illegal behavior is particularly blurred with regards to phone, SMS, email and other telecommunications records, as the laws regulating the privacy of this type of information vary from one state to another in the U.S. and from one country to another, worldwide. The Federal Trade Commission (FTC) has attempted to bar pretexting for telephone records under Section
5 of the FTC Act (which bars "unfair or deceptive acts" in business practices) and has filed several lawsuits against online data brokers to that end. The FTC recommends that individuals never out personal information on the phone or over the Internet unless the individual has initiated the contact.

In a high-profile case, a firm contracted by Hewlett Packard Chair Patricia Dunn used pretexting to access telephone records of HP's board of directors. Dunn engaged the firm to investigate board members after insider information about HP's long-term strategic plans appeared on News.com.

This was first published in May 2011

Continue Reading About pretexting

Here's the FTC's Web page on the pretexting provisions of the Gramm-Leach-Bliley Act.

The New School of Information Security
This article from Time, "Are the Police Digging into Your Phone Records?," examines the potential intersections between law enforcement and online data brokers.

- This USA Today article describes a real-world example of pretexting at HP.
- Here's a FAQ from News.com explaining the pretexting scandal at HP.
- Here are 8 ways to defend against pretexting from eWeek.com.

Glossary

'pretexting' is part of the:

- Application security Glossary
- Security management Glossary
- Security threats and countermeasures Glossary

View All Definitions
Related Terms

**consumer data**
Consumer data is the information trail customers leave behind as a result of their Internet use. See complete definition

**field-level encryption**
Field-level encryption is the ability to encrypt data based on entire fields. See complete definition

Dig deeper on Enterprise data security and privacy

North Korea behind Sony attack -- what now?

How is the Sony hack different from other attacks?
Cyberattackers breach USPS security, but what were they after?

Load More

0 comments

Share your comment

Register or Login

E-Mail

email@techtarget.com
Top 10 governance, risk and compliance strategy articles of 2014

In our “Top 10 of 2014,” find the most popular SearchCompliance articles from the past year offering advice on deploying a ...

Active defense: The perils of cybervigilantism

Legally ambiguous active defense strategies are risky -- and costly -- for businesses, but could the benefits outweigh the ...