Security Awareness: Social Engineering.

You get a phone call from someone saying they're from the Security and Fraud department at VISA. They believe your card has been used for fraudulent purchases. They give you the card number, your name, maybe even your address. "In order to verify that you are still in possession of the card, could you please give me the 3 digit security code number on the back of the card." You think that if they have all that other information, they must be legitimate. They assure you that the charges will be reversed, and if you have any questions, feel free to call back at the anti-fraud phone number. They might even give you a case number. Unfortunately, it's a scam. The security code on the back of your credit card is the last piece of information they need to use your card for internet purchasing.

This is Social Engineering, and it's very real (http://www.snopes.com/crime/warnings/creditcard.asp). Now, for a definition. Webopedia (www.webopedia.com) defines Social Engineering as: "…the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful."

Social engineering certainly isn't new. It's just become more prevalent in the age of computers and instant access to data. Sometimes the information being requested seems harmless, even useless. The type of information requested could vary greatly, depending on what the scammer is trying to do, and how much information they've already obtained. They might be asking for birthdays, mother's maiden name, etc. After they are done collecting this seemingly innocent information, they will have enough to gain unauthorized access.

The thing to keep in mind is that identity theft isn't the only thing someone might be after. With enough information, someone could get a "head start" on guessing passwords, or gaining unauthorized access to a restricted area, or having a password reset by providing credentials (mother's maiden name).

The best defense against this type of scam is to simply be aware it can happen, and always be skeptical. Verify the identity of the person asking for sensitive information. Check their identification, or even check the caller ID. If you're unsure, ask your Manager. Never assume that the person requesting information is legit, or whom they claim to be. Never be embarrassed to challenge someone who's asking for information. If they are legitimate, they won't mind.

If you have any questions about this, or any other type of suspicious activity, contact ITSecurity@hofstra.edu.