Project Title: Does Level of Risk Affect Individual Computer Security Decisions?

Project Description:

Theory

Individuals make many decisions involving the security of their computers and their various online accounts. These decisions often have immediate personal implications and frequently have somewhat less obvious social effects as well. Even those who ignore computer security entirely are effectively making the decision to go with whatever default security their operating systems, programs, and behavior provide – presumably because they would rather spend their time thinking about other things.

Normative models of choice such as expected utility theory and even descriptive models such as prospect theory assume that individuals simply weigh the personal costs and benefits when making their security decisions. They would consider factors such as the following:

- the cost of securing themselves
- the loss if their computer or account is compromised
- the probability of being compromised if not secured
- current income or relevant reference point

Theoretically this seems sound, but empirically I have found no work verifying that individuals actually consider any of these factors.. As a society with a growing concern for security and privacy on the Internet who engineer networks and software to understand more about what influences individuals' security decisions. Further, since the individual security decisions can sometimes have social implications policymakers should also be quite interested in this decision process.[1]

I propose a study to specifically determine if the degree of personal loss to the user resulting from being compromised will, ex-ante, affect the user's amount of investment in security.

Main Hypothesis – I hypothesize that higher potential for personal loss results in higher degrees of investment in security. As such, students whose W-2 tax forms are stored online at the University (and thus subject to risk of identity theft) will change their passwords more frequently than students who's W-2 tax forms are not (all else equal).

Auxilliary Hypotheses I can test with the data –

[1] *For example, computers infected with a virus can be used in costly DDOS attacks or as part of Phishing/identity theft networks. Or, when an individual's credit card identity is stolen, society pays the price in the form of higher interest rates to cover credit protection costs.*

1) Individuals who have higher levels of network access/security clearance will be more diligent about changing their passwords, all else equal.
2) Individuals who are in positions to know more about computer related risk (for example, computer science majors) will be more diligent about changing their passwords than those who are not, all else equal.

Strategy

At U.Penn, some graduate students are employees and are paid wages or a stipend on a monthly basis while some receive no income from the University. Students who are paid now have their W2 income tax forms accessible online through their Penn ID and password. All students have a Penn ID and password used to access student schedules and transcripts, but only employees can also access their W2 forms with this information.

W2 forms contain social security numbers, birth dates, and all of the information necessary for identity theft. If the Penn ID/password of a monthly paid student were compromised by a thief, the thief could use the information from the W2 to open a credit card in the name of the student and make purchases. The student, upon discovering this, might be responsible for some or all of the charges depending on credit protection, but he would certainly be entangled in a time consuming mess to get everything sorted out.

It is well established (and frequently advised) that changing one's password frequently greatly increases the security of an online account.

I will test my hypothesis using a dataset in which each observation will be an individual PennID user and will include the following

- Number of password changes made in a given period by the individual
- Whether the individual's W-2 is online
- Number of times the individual accessed his W-2
- Age
- Status (undergrad, grad, professional student, faculty, staff)
- School, major, or department
- Self identified race/ethnicity
- Permanent home address

If individuals weigh their own level of risk in their security decisions, then PennID users whose W-2 forms are online will be found to change their passwords more frequently (all other things equal).

Motivation

While it is hoped that this paper would have general implication about individuals perceptions of computer risk and security decisions, at the very least it will tell us something about online account security and identity theft. Many financial institutions

have significant costs to cover or prevent identity theft and currently seek information on affects the security decisions of their users. If this study confirms that the potential for personal loss affects individual computer/account security decisions, then that is evidence that there is some sort of rational (or at least partly rational) decision process in users' minds – something as yet unproven. It would also indicate that increasing the cost of a security failure to the user (with perhaps fines or punishments) would induce increased investment in security – this is particularly important when there are interdependent security risks or when there are social costs to an individual security failure.

Primary Faculty Member: Dr. Howard Kunreuther

Primary Faculty Member Signature: