What Is Sensitive Data?

Sensitive data encompasses a wide range of information and can include: your ethnic or racial origin; political opinion; religious or other similar beliefs; memberships; physical or mental health details; personal life; or criminal or civil offences. These examples of information are protected by your civil rights.

Sensitive data can also include information that relates to you as a consumer, client, employee, patient or student; and it can be identifying information as well: your contact information, identification cards and numbers, birth date, and parents’ names.

All of this data belongs to you. You have full rights to access and use this information and you also have rights to know how others are doing the same. You should be protective of this information, just like you would be of your other belongings.

Why Data Needs Protecting

With the advent of the Internet and new technologies that allow easier, quicker, as well as anonymous access to more information than ever before, people have now become more aware of identity theft and make conscious decisions on how to protect themselves.

If the information is sensitive, it’s likely to be protected by laws, regulations, or policies. However, you can take an active approach to making sure your information has not fallen into the hands of those who would misuse it for financial gain or other reasons. Identity theft and online crime have now surpassed any other form of crime in profits earned, including drug-related crimes, so it is important to be wary of how exposed your information really is.

Protecting Financial Information

Below are some tips to minimize the exposure of your personal financial information.

- **The Internet:** Know with whom you’re doing business, especially when you provide financial or identity information. Only deal with web sites that provide secure web pages, i.e., those addresses that start with “https” rather than “http,” for your transactions. Legitimate sites will provide contact information and signed certificates for your verification. When logging in to financial accounts, use a strong password that you change on a regular basis.

- **Credit cards online:** Consider designating only one of your credit cards for online purchases. If a problem occurs with that card, you can cancel it and still have other cards. You can also request that your credit card limit be set to a level consistent with your credit card activities (rather than the high line of credit the company assigns). But, don’t set it so low that you’ll have to use a second credit card.

- **Credit card receipts:** Always check your credit card receipts and other financial paperwork. They should not have the complete credit card number listed, only the last four digits. If the full number is listed, ask that it be truncated in the future.

- **Your credit report:** You should get a report at least once a year. Federal law entitles citizens to a free credit report per year from each of the three national credit bureaus. If you think you are in a high-risk category for identity theft, be sure to get a copy of your credit report once every three months.

To keep a close watch on your personal financial data, request a report using the contact information listed on the back of this pamphlet.

How Is Data Exposed?

Here are three ways your data can be exposed:

- **Intrusion:** Intruders can gain access to your data through a weakness in your computer system. To protect against this, keep your operating system updated, and use virus protection and strong passwords.

- **Phishing:** This is a clever method of extracting information from unsuspecting individuals. An e-mail, designed to look like it originated from a reputable company, usually a bank or online store, will tell you that there is a problem with your account. If links appear in this kind of e-mail message, never click on them regardless of how “believable” they seem or who the source is. If you have an account with the organization, it’s better to call your service representative and verify the authenticity of the e-mail. If it is legitimate, ask to complete the process by phone. This eliminates the need to send your sensitive data over an unprotected network connection. To learn more about phishing attacks, go to http://www.antiphishing.org/.

- **Social Engineering:** Sometimes swindlers attempt to gather sensitive information, such as birthplace or mother’s maiden name, by posing as a representative of a legitimate organization. You should always be wary of unsolicited requests from your bank or financial institution in which you are asked for information that could potentially be used for fraudulent purposes. IS&T never asks you to provide your username and password in e-mail or over the phone.

For links and further information, see the rear panel of this pamphlet.
Learn more:

Credit Reports:
Equifax
Order reports, call 800-685-1111.
Report fraud, call 800-525-6285.
http://www.equifax.com

Experian
To order a report or report fraud, call 888-397-3742.
http://www.experian.com

TransUnion
Order reports, call 800-888-4213.
Report fraud, call 800-680-7289.
http://www.transunion.com

The FTC:
Federal law on free annual credit reports:
http://www.ftc.gov/opa/2004/06/freeannual.htm
Identity theft:
http://www.ftc.gov/idtheft

Quiz for Identity Theft Risk:
Use a simple quiz to determine what your identity theft risk is.
http://www.privacyrights.org/itrc-quiz1.htm

IT Security at MIT:
Website:
http://web.mit.edu/ist/topics/security
Pamphlets:
http://web.mit.edu/ist/topics/security/pamphlets.html

Newsletters:
Safe Computing Column (IS&T Newsletter)
http://web.mit.edu/ist/istnews
IS&T Security FYI (Subscription email newsletter)
http://mailman.mit.edu/mailman/listinfo/ist-security-fyi

The Safe Computing Pamphlet Series
This pamphlet, from the IT Security Support Team, is one in a series. The series is designed to help you make your computing environment safer and protect your data from inappropriate disclosure and use.

Computing Help Desk
computing-help@mit.edu

IT Security Support
security@mit.edu

© 2008 Massachusetts Institute of Technology