Q&A on Information Technology Security

1. What can I do to keep my user accounts (e.g., email, Banner, etc.) safe?

There are various things that you can do to help keep your user accounts secure.

- One important component of maintaining the security of your user account is to maintain the security and secrecy of your user account password. University policy already requires that you update your UD user account passwords at least twice a year, but quarterly is even better. You can also maintain the security and secrecy of your passwords by following password construction guidelines and password protection guidelines.

- Another important component of maintaining the security of your user account is avoiding or preventing what are referred to as "social engineering attacks."

2. What are password construction guidelines?

Password construction guidelines identify what types of passwords are likely to increase the security of your user account, and what types of passwords are likely to decrease the security of your user account. In general, you should seek to have strong passwords, rather than poor or weak passwords.

3. What are characteristics of poor or weak passwords?

Poor or weak passwords frequently have one or more of the following characteristics:

- The password contains less than eight characters;
- The password is a word found in a dictionary (English or foreign);
- The password is used for more than one University of Dallas or non-University of Dallas account; or
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.,
    - Computer terms and names, commands, sites, companies, hardware, or software;
    - The words "University of Dallas", "dallas", "ud" or any derivation;
    - Birthdays and other personal information such as addresses and phone numbers;
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;
    - Any of the above spelled backwards; or
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

4. What are characteristics of strong passwords?

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Are at least eight alphanumeric characters long;
- Are not a word in any language, slang, dialect, jargon, etc.; and
- Are not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

5. What are password protection guidelines?

Password protection guidelines include various practices that are likely to increase the security of your passwords, and consequently your user accounts. For instance, the University's recommendation that you change your password every quarter is designed to crease the security of your user accounts. Other password protection guidelines include:

- Do not write down your passwords or store them online. If you must store your passwords electronically, be sure that they are stored with encryption.
- Do not use the same password for more the one user account.
- Do not share your passwords with anyone, even the IT Office. No one else should need to know your passwords.
- If you suspect that your user account or password may have been compromised, report the incident to the IT Office and change all of your passwords.

6. What is a "social engineering attack"?

A social engineering attack is a method of gaining access to user accounts or confidential information by way of an error or mistake made by the authorized user. Whereas some attempts to attack information systems are based primarily on the use of technology, a social engineering attack primarily makes use of non-technological means, such as lying to users, impersonating individuals with authority (e.g., an IT Office or supervisors), tricking a user into doing some that makes their system vulnerable, offering bribes, or making threats, including threats of blackmail.

7. What can I do to avoid or prevent a social engineering attack?

First, the IT Office provides training and guidance so as to avoid and prevent social engineering attacks. Be sure to diligently attend and listen to any such training and guidance.

Second, there are warning signs of a social engineering attack. If you see any of the following warning signs, immediately notify the UD IT Office at support@udallas.edu:

- You receive an email or other communication that includes a reference to a higher authority figure (e.g., a supervisor), but the email or other instruction does not contain any documentation or confirmation that it is from the authority figure;

- You receive an email or other communication with a claim or urgency or emergency, but without contextual support;

- You receive an email or other communication with a request for unauthorized, undocumented release of information, particularly of passwords, sensitive personal information, or financial information;

- You receive a communication from an unknown individual via phone, email, text, fax, or in person (an 'unknown individual' may include individuals who purport to be reporters or alleged subcontractors of the University); or

- You receive any appeal for information without proper documentation or approval.