

Social Networking

Deborah Schroeder

Assistant Vice Chancellor Information Technology

Social Networking

- Humans are a weak link in cyber-security and can be easily tricked
- Falling for an online scam or hack can be damaging to the individual as well as the organization s/he works for
- Risks include:
 - Spreading malicious code
 - Compromising computer
 - Accessing personal information



Social Networking Threats

- Malware embedded in a website or third party application can infect millions of computers when a link is shared.
- Tools to take control of a user account and access contact data or private data.
- Social engineering attacks.
- Identity theft.



Social Networking-Why Worry?

- When information is posted to a social networking site, it is no longer private.
- The more information you post, the more vulnerable you become.
- Even with high security settings, friends or websites may inadvertently leak your information.



Social Networking-What Happens?

- Personal information you share can be used to conduct attacks against you or your associates, not necessarily via social networking.
- The more information you share, the more likely someone could impersonate you and trick a friend into sharing personal information, downloading malware, or providing access to restricted sites.