Facebook Fiasco

"A friend loves Facebook and she shares the smallest minutiae of her life with her friends. Once, she was having a bad day at work and posted how stressful her day had been and how awful her boss was. Because of privacy settings, her boss saw the post. Thankfully, he was nice and only mentioned it to her in passing, but what if her boss hadn’t been forgiving?"

Do you have stories like this one?

The latest census shows 70% of homes in the U.S. have a computer with Internet access. We all have challenges with technology. What have you learned? Tell your co-workers about your experience – it could help them.

Pass it on: Send your story to story@sp.providence.org for publication in our newsletter and receive a gift!

How your privacy may be compromised

We love our social networking tools. Unfortunately, so do cybercriminals. Remember that everything you post is public information.

Check your privacy settings and follow these safety tips:

• Once compromised, social media accounts are targets for phishing scams. If you receive a suspicious message from a social network connection, delete it immediately.

• Always think twice before posting details about your work day. HIPAA rules also apply to social networking situations and it is never appropriate to post any patient information.

• Don’t trust a message just because it looks professional. If you’re interested in a message because of its content, Google it separately.

• When accepting friend requests choose wisely, they will see everything you post – and so will their friends.

Tweets, posts, and updates

Talking to your friends: Which of these posts/updates is too much information (TMI)?

1. Our cat finally came back.
2. Looking forward to our family vacation in Disneyland next week!
3. Good news from the ER – our new mayor is the proud daddy of twins!
4. I won the cookie contest!
5. I just heard Justin Bieber died.

How your privacy may be compromised

We love our social networking tools. Unfortunately, so do cybercriminals. Remember that everything you post is public information.

Check your privacy settings and follow these safety tips:

• Once compromised, social media accounts are targets for phishing scams. If you receive a suspicious message from a social network connection, delete it immediately.

• Always think twice before posting details about your work day. HIPAA rules also apply to social networking situations and it is never appropriate to post any patient information.

• Don’t trust a message just because it looks professional. If you’re interested in a message because of its content, Google it separately.

• When accepting friend requests choose wisely, they will see everything you post – and so will their friends.