Social Media & Cyber Security

ITS | Infrastructure Technology Solutions

Are you aware of how much of your personal data is shared when you use social media, and do you know who has access? Learn how to safeguard your accounts!

Social media can be a great way to stay connected personally and professionally. Recent security breaches at Facebook and GooglePlus, along with government investigations and hearings related to social media privacy and data collection, have given some users pause when interacting on social media. Have you checked your accounts to make sure you aren't over-sharing or over-connecting?

General Tips:
Use a unique password for every social media site.
Keep your phone and your computer locked with a passcode, and if using a shared computer at home, consider setting up different user profiles on the machine to avoid logging into social media accounts from the same browser. Always lock your computer and your phone when not in use.
When accepting friendships, be choosy. Consider deleting requests if you don't already have a personal connection outside of social media.

Photos:
In every platform, check the background of photos before posting - especially if posting from work. Are there sticky notes with passwords exposed in the photo? Are there open screens/tabs on your computer that would be problematic if shared online? Are there items in the background of the photo that demand a retake?

Away Status:
Finally, if you don't leave a note on your physical door to notify visitors that you are away, then you shouldn't use social media to broadcast your away status. Consider radio silence when on vacation, or at least check to make sure posts and photos are only shared with friends if you can't wait until your return flight to post them.

Facebook:

Security & Login: Several settings in this menu help you keep your account safe. The "Where you're logged in" section allows you to log out of any locations currently logged in - it's important to check this periodically and especially when there have been data breaches. Logout any sessions that are not recognized.

Apps & Websites: check this list to see what third-party apps and websites also have access to your facebook account credentials and data.

Account Details: Attackers can use public details from your account to socially engineer you or your employer, or use data to create loan applications, etc. Don't list your full birthdate, and think twice about listing your hometown if that is also the location of your birth.

Timeline and Tagging: Check these settings and make sure they only allow access to the groups of people that you want to connect with: Friends? Friends of friends? Everyone in the world?

LinkedIn:

Full Resume: If you aren't actively job-seeking, consider removing some details from your resume to prevent an attacker from mining data that they could use to complete loan/financial applications.

Snapchat:

Contact info: Be selective about sharing your Snapcode and username. Consider removing your listing in the Quick Add settings to allow only close connections to friend request you.

Permanence: We should never assume that Snaps are deleted or not captured; there are apps that allow contacts to screenshot your contact without notifying you, and Snapchat stores your content on their servers long after the Snap expires on your device.

www.iowadatacenters.com | 319-465-4463 | info@iowadatacenters.com
22068 Business Highway 151, Monticello IA 52310

Managed Helpdesk/IT Services, Wired/Wireless Networks, Hosting Services, Physical Security