A4TD ASSOCIATES FOR TRAINING & DEVELOPMENT
ADVANCING WORKFORCE DEVELOPMENT FOR MATURE WORKERS SINCE 1983

Network to Work Meeting - January 2021
RESOURCE DOCUMENT #1

Protecting your Privacy and Identity While Using Social Media

Social media sites like Facebook, Instagram and LinkedIn are by design intended for sharing more information – and being more social – than traditional methods of communication. Furthermore, not only are you putting more information on the internet about yourself, but you are also influencing how people perceive you by what you post.

Therefore, it is important to be very mindful and cautious about what you share through social media.

It is equally important that you understand and use the best practices and website tools that can help you protect your privacy and your identity.

So here are some things you can do to use these social media platforms in the safest way.

Ways to Protect your Identity on Social Media:

1. **Don't share your personal information publically; keep it private**. Provide as little personal information as possible. Consider changing a few details so those who can access your details won't have your actual information to use for identity theft-related activities. For example, if your birthday is June 15, you might list it as June 3 or July 1.

   When asked to provide "about me" information, treat these requests as optional. This information includes:
   a. Your birthday, including the year
   b. The name of your high school
   c. Your home address and phone number
   d. Your hometown
   e. Your email address

f. Your social security number (never provide this online unless you are on a secure and trusted site that you are familiar with such as SSA.gov)

g. Your driver's license number (never provide this online unless you are on a secure and trusted site that you are familiar with such as your Department of Motor Vehicles)

h. Pet names

i. Your current city (list just your state, or a more general statement like "the Albany NY area" instead)

2. **Set strict privacy settings on your social media accounts** so that your personal information is private or only visible to your friends.
   a. Explore all of the privacy settings for the platforms you use.
   b. Check these often as the social media platforms regularly change their settings.

3. **Know the people you connect with as Friends or Connections**.
   a. If you friend someone you don't know, it makes it easier for them to access your information and use it to find out more about you. This makes you more at risk for identity theft.
   b. Use the "decline" button to refuse friend or connection requests.
   c. You can choose to unfriend, unfollow, unconnect or block anyone you no longer wish to be connected with.
   d. Watch out for fake accounts set up by "bots" or fraudsters. These are created for a variety of negative purposes including to run scams, collect your personal profile information, or to provide disinformation.

4. **Always log out of your social media account,** especially when using a public computer at a library or Career Center, or when using a computer belonging to a family member or friend.
   a. Logging out prevents others from taking over your social media profile and then changing your personal information, attacking your friends, or even locking you out by changing your password.

5. **Use a variety of strong passwords and change them often**. Combine upper and lower case letters, symbols and numbers. Ten characters or more is ideal.
   a. Don't use the names of your pets or family members, or birthdates, anniversaries, etc.
   b. TIP: select a phrase or song lyric that you can easily remember and use the first letter of each word.
   c. All of your passwords should be different and obscure.
   d. Don't share your passwords.
   e. Change your passwords frequently.
   f. Have a password lock on your phone.

g. Use two-way authentication when offered as an option; this requires you to provide a secondary piece of information to log into a site.
h. If given the choice, ask to receive an email notification for every log in to your social media account.
i. Consider using a Password Manager for your web browser. It saves all of your passwords in an encrypted database and fills in the information for you. All you need to remember is the master password for your Password Manager.

6. **Use Internet Security Software such as Norton**. This can protect you if you click on a link that contains a "malware" program designed to steal your personal information from your computer. These links often come disguised as a message from a friend.

7. **Don't tag or post your specific location**, or "check in". This can make it easier for criminals to know when you're not home.

8. **Google yourself from time to time**. This will give you an idea of what information about you is currently available to the public.

9. If you use a platform like Facebook, **review your "tags" setting**. You can set it up so that you can view any post you are named in and then decide if you want it to be shared with others.

10. **Be thoughtful about what you post.**
    a. Your friends, connections and others with access to you posts and photos can download them or otherwise copy them. This means they may remain online even after you delete them. So, be very cautious about what you post.
    b. Don't share anything that you wouldn't want your beloved family member to see. Assume that others can find anything you share online forever.
    c. Be mindful that your employer or co-workers may be able to see what you post on social media.

11. **Be aware of "phishing" scams.** Phishing is when someone poses as a legitimate organization or a friend and contacts you using your public information such as your phone number, email, or text. They do this to try to trick you into providing sensitive data such as your credit card or bank account numbers and passwords.
    a. Don't open or reply to suspicious emails or messages
    b. NEVER click on links that have been sent to you. Instead, use your search engine to look for the legitimate website referenced in the email or link.
    c. If you do click on a link and are taken to a website asking for your personal information, don't provide it.

    d. If you receive a message from a friend, your bank or your credit card company, for example, that you are unsure about, contact them directly to see if they sent the message.
    e. Common examples:
        i. Emails saying your Amazon account is frozen and you need to update your information, including payment information.
        ii. Facebook friend requests from people who are already your friends. Their accounts may have been hacked.
        iii. Romance scams
        iv. Opportunities to make money by providing personal information.

12. **Inventory your social media accounts.** This includes old ones you haven't used in years. Try to delete old accounts or remove posts you don't want others to see.
    a. Most websites have account recovery options if you can't remember your account information.

13. **Use only reputable websites when making online purchases.** To be sure the website uses a secure, encrypted connection for your personal and financial information, make sure the web address for the webpage asking for personal or financial information starts with https: (the S is crucial)

14. **Don't allow the social media site to provide your personal information to third-party apps or marketing agencies.** Criminals can also obtain your personal information through third-party applications. Most social media sites have apps that ask for permission to access your account information before you can install them. Don't grant this permission. This is one way hackers steal your details to commit fraud.

15. **Regularly check your credit report** for suspicious activities involving your name.

Review and Control your Privacy Settings

When you set up an account with LinkedIn, Facebook, or any other social networking site, you can use that site's privacy settings to control who sees your information. ***See Resource Document #2 for visuals that will guide you to review your settings on these sites.***

LinkedIn:

LinkedIn allows you to adjust your privacy settings to control how much of your information can be seen by others. You access these privacy settings from the main menu. Click on the arrow next to the "Me" icon. Then, from the drop down menu, click on "Settings & Privacy". Here you can control the information you provide and how you will interact with LinkedIn. All changes you make are saved automatically.

Facebook:

Some people use Facebook strictly to share information with family and close friends. Others enjoy putting themselves out there and networking with a broad audience. There are three places in Facebook where you can control your privacy settings.

1. In "Privacy Settings and Tools"
2. On your individual posts
3. On your profile

In these locations you can decide if you want your information, newsfeed, photos and other information to be shared with the public; with your friends and their friends; with only your friends; only with you; or shared in a custom manner. Here is a bit more about your sharing options:

1. **Friends**: Item is seen by your friends but not shared with people you don't know;
2. **Lists**: If you group your friends or connections into lists, only the people on the selected list will be able to see what you post.
3. **Friends of friends**: Your friends see what you post, and it can also be seen by their friends. This could include people you don't know and even friends you deliberately blocked or unfriended.
4. **Public**: Least secure. Allows anyone on Facebook and even on the web to see what you post. It also opens you up to third party applications and advertisers.
5. **Only Me**: only you can see what is posted on your timeline, including photos you have been tagged in. This way you don't have to worry about others seeing anything embarrassing showing up on your profile.
6. **Custom**: You can decide more specifically who gets to see certain information such as your contact information.

Sometimes a website – Pinterest, for example – may allow you to log in using your Facebook account and login credentials instead of creating a new account (user name and password). This is called "the Facebook Platform" and it can affect your privacy in different ways. Some sites use this to connect your account to their services. Others will customize your experience based on your personal information. The Facebook Platform lets other websites connect with your Facebook account and view your public information. ***The safest approach is to create a separate, strong password and user name for each of your social media accounts.***

Always read the information provided by the site about how they will use your information – including their privacy policy – and don't agree to anything you aren't comfortable with.

Best Practice: Go into Facebook's "Privacy Settings and Tools" and review your settings. You should consider limiting who see things to your "Friends". This limits who can see your information and posts.

Remember, if you select "Public", anyone with a Facebook account can find and view your information, posts and activities. This includes your personal information, posts, photos, comments, and unflattering posts. Third party websites and applications can also access your information.

Sources:

"Internet Safety – Social Media Privacy Basics", GCF Learn Free tutorial,
https://edu.gcfglobal.org/en/internetsafety/social-media-privacy-basics/1/

"LinkedIn Basics – Adjusting Your Settings and Privacy on LinkedIn
https://edu.gcfglobal.org/en/linkedin/adjusting-your-settings-and-privacy-on-linkedin/1/

"Facebook – Adjusting Your Privacy Settings
https://edu.gcfglobal.org/en/facebook101/adjusting-your-privacy-settings/1/

"Privacy on Social Media Guards Against Identity Theft", by Julie Myhre
https://www.businessnewsdaily.com/4194-social-media-security-tips.html

"10 ways to protect yourself on social media", by Concordia Social Media Team, November 21, 2017.
https://www.concordia.ca/cunews/main/stories/2017/11/21/stay-safe-on-social-media.html

"How to Keep your Personal Information Safe on Social Media", by Norton Lifelock
https://us.norton.com/internetsecurity-how-to-how-to-keep-your-personal-information-safe-on-social-media.html

"How to Protect Your Privacy on Social Media", by Stefan Lembo Stolba, Experian, May 29, 2020.
https://us.norton.com/internetsecurity-how-to-how-to-keep-your-personal-information-safe-on-social-media.html

"How Can I Protect Myself from Identity Theft Online?", by Webroot, an **opentext** company.
https://www.webroot.com/us/en/resources/tips-articles/how-can-i-protect-myself-from-identity-theft-online

"Identity Theft Through Social Networking? Lessons to Take Now!", by Joy Mali, Lifehack.org
https://www.lifehack.org/articles/technology/identity-theft-through-social-networking-lessons-take-now.html