NATIONAL CYBER SAFETY AND SECURITY STANDARDS

एनसीएसएसएस

Security Precautions – We should keep in mind when using Social Networks/Media

- Social networking means opening up and sharing information online with others, but there's some information you should never share online.

- Never use the same passwords that you use at work on a social networking site.

- Limit the amount of identifying information you use, like your birth date, address, full name, etc. (This step can also help prevent identity theft.)

- Limit usage of social networking sites to personal use only. Do not write about work issues. Always assume everyone in the world will be able to see what you're writing even if the site limits your post to your friends exclusively.

- Try to avoid mentioning where you work; so that if you mention something you thought innocent (but that might be valuable information for hackers) they will not know who to target.

- Be wary of what you're posting, if you use your pet's name as a password anywhere do not post about it on your social networking sites naming it.

- Do not log on to your social network page from public computers such as internet cafés where someone might have installed a key logger and would later get access to your credentials.

- Do not automatically trust that posts are from who they claim they are; if your workmate sends you a private message asking for some confidential information first verify that he/she did really send you that message as their account might have been compromised.

- Do not send confidential information through a social networking site even if someone who has legitimate access to that information asks you to.

- Beware of what links you click and what software you download and install. Do not trust links/software sent by your friends implicitly as they themselves might not be aware it includes malware or their account might have been compromised.

- Always be cautious on Social networks. If someone asks to be friends on a social networking site and the profile appears to match a work mate, check personally with that person before accepting him as he could be an imposter. Also be skeptical of any offers or prizes you might have been told you won, they might actually be phishing attacks.

- Ensure your computer is up to date and has good antivirus protection; social networking sites are frequent targets of malware attacks.

- Protecting yourself from sharing Too Much Information (TMI) can save you from identity theft and even protect your physical safety. So let's start with the obvious … never share your AADHAR number (including even just the last 4 digits), your Birth Date, Home Address or Mobile number. Of course, you should protect all of your passwords, PIN numbers, bank account and credit card information.

- Don’t assume you have to take whatever Default Privacy Settings the site gives you. Check out the settings, configuration and privacy sections to see what options you have to limit who and what groups can see various aspects of your personal information.

- Check the privacy settings for each of your accounts, and make sure they are all set to private. Better you are ensure that only your ‘Friends’ or ‘Followers’ who have accepted your request, can see your posts, including photos and videos.

- Keep personal details such as your address, email address, phone number and birth date private.

- Be mindful that ‘Friends’ or ‘Followers’ may take screenshots of your posts, or save photos and videos and share them with others. Don't post anything that may put you in danger, affect your reputation or be used against you or your family.

- Be careful how much information is in the photos or videos you share. For instance, could someone find out where you are if you are pictured at a well-known venue or someone’s house?

- Be careful who you become friends with online and what you share with them.

- Be wary of surveys and competitions. Sometimes they ask for your personal details and you might be tempted to take them if attractive prizes are on offer. Often these scams are linked to identity theft.

- Regularly check your settings. Be aware that updates to software can change your privacy settings, making them more public than you would like.

- If you don’t want people to know where you are, disable the location services on your device and avoid ‘checking in’ to places and venues. Ask your friends not to check you into places as well.

- If you have a friend who's at risk of violence or stalking, don't ‘check in’, ‘tag’ or post anything about them publicly.

- Change your settings so others can't ‘tag’ you or ‘check you’ in without your okay.

- Don't hashtag anything you don't want to become public. Anything with a hashtag (such as #havingagreattime) is searchable on the internet, depending on your privacy settings.

- Facebook probably has some of the broadest privacy options, giving you control where no one, friends, friends and networks, or everyone can see basic info, personal info, photos, friends and postings.

- Search is a new area where users are gaining control of what others are allowed to see. Some sites let you set limits on who can see search results about you on the social networking site.

- If you've just joined a social networking site, or even if you have been a user for some time, log onto your account and view and adjust the privacy settings –new settings are often added over time.

- Be careful about what you post! Consider the articles you post to your profile, the pictures you put in an online album, or any status updates that indicate where you are at the moment (such as "checking in" at a restaurant) or where you are headed (such as a vacation destination). These types of posts can reveal a lot about you: your interests, your whereabouts, and your future plans, which can lead to someone finding you.

- Log out of your account by clicking "log out" after each session on your social media page. Do not simply close the browser, as it does not always log you out of your account, which would then be viewable by any other user of the computer.

Safety advice for women who experience violence

- This advice has been developed for women who have experienced violence or fear they may experience violence to themselves or their children, including cyber stalking, from a current or former partner or another worrying person.

- Turn location services off in the settings of all devices you use and check the privacy settings on all social media. This will limit others tagging you or posting photos or videos of you. Do the same with children's devices and accounts.

- Consider minimizing social media posts until you feel safer. If this will make the abuser suspicious then keep posting but without location information or anything that will upset them.

- Do not post photos or videos that show your location or the location of your children. Abusers may identify patterns in your day and week. Cut off the information so they can't follow you.

- Talk to your children about how important it is not to put location information online. Include them when you are developing the safety plan so they can communicate and stay connected safely.

- If there is any direct abuse or threat contact the police for advice. Ask police what evidence they will need to prove a crime is being committed.

Safety Measures at LinkedIn– Limit work history details on LinkedIn

- Would you put your full resume online for everyone to see? Probably not. It would be too easy for identity thieves to use the information to fill out a loan application, guess a password security question (like hackers did with VP candidate Sarah Palins' Yahoo account) or social engineer their way into your company's network.

- Limit your work history details on sites like LinkedIn. If you feel you need the added information to help in a job search, expand the details during the job hunting process and then cut back later after you have a position, leaving just enough information to entice recruiters to contact you with interesting new positions.

- LinkedIn also offers some capabilities to restrict information. You can close off access by others to your network of contacts, something you don't have to share if you don't want. This is a common practice by sales professionals and recruiters not wanting to expose their valuable network to others who might poach customers or prospects from them.

Safety advice for Women & Children who experience abuse on social media

- If you are being seriously threatened and you feel that your life, or your children's lives, are at risk you should report to the nearest Cyber Police Station.

- Do not respond to the abuse. Keep evidence of the abuse such as a screen shot or photo with your phone. Find out how to take a screen shot as the evidence may be useful later if you want to take legal action. It's a good idea to keep all evidence in a safe place or consider sending it to a friend for safe keeping.

- Reporting the abuse to the website it was posted on is a good first step to take, unless this will make the abuser angrier and put you in greater danger. To see instructions on how to do this, visit our Social media page and select the relevant social media service.

- If you can, block the person and ignore their posts. Again, only do this if it is safe and won't make the abuser angrier.

- Tell a trusted friend. You may feel awkward about this but it is a good thing to share your concerns with others who care about you. Seeking help is your right and it could mean the abuse stops more quickly.

General Safety Strategies:

- Stop all contact and communication with the person stalking or harassing you but keep any evidence of the stalking (such as voicemails, texts, emails, etc., for future court cases or criminal actions). Responding to the stalker's actions may reinforce and/or encourage his/her behavior.

- Carry a cell phone with you. Keep handy or memorize emergency phone numbers that you can use in case of an emergency. If you ever feel you are in immediate danger, call local women helpline number.

- Trust your instincts. If you feel uncomfortable for any reason, you may want to reach out for help, even if nothing immediately dangerous is happening.

- Have a safe place in mind to go to in an emergency. You might go to a police station, place of worship, public area, the home of a family member or friend (unknown to the stalker), or a domestic violence shelter. If someone is following you, it is generally not a good idea to go home.

- Try not to travel alone. If you run or walk for exercise, you might want to get an exercise buddy to go with you. Always vary your routes to and from work or school, the grocery store, and any other places regularly visited. By changing your daily routes, it could make it more difficult for someone to learn your routine – however, also be aware that a stalker may put a GPS monitoring device on your car or cell phone. One hint that a GPS device may be installed is if you are varying your routes or going to unexpected places but the stalker still seems to find you.

- Be aware of how much identifying information you are posting on the Internet through social networking sites and online purchases. You may want to select the highest security settings on any social networking accounts and think carefully before giving out your personal information through online purchases.

My account has been hacked. What should I do?

- Change your password immediately. If you are still worried, start a new account.
- If you can't get into your own account, you need to report this to the website.

Someone has set up a fake social media account in my name

- You can report the fake account directly to the website that hosts it. Be aware though that it can take some time before the fake account is removed.
- If the account is abusive or threatening, keep evidence of the abuse.
- Contact local police to find out what evidence they need, and report the abuse to them if you are scared about your safety.