Safe Social Media Use

Social media platforms like **Facebook** and **Instagram** allow us to stay connected with friends and family and share what's going on in our lives. They're great fun, but it's important to **use privacy settings** and **be careful about what you share** to protect yourself.

Lock down your privacy settings: On Facebook, check your **Privacy Settings** (find the Privacy Checkup tool) to make sure your posts are only visible to your **Friends**, not the whole public. You can control who can see your information. For example, you might set your profile details (like your hometown, email) to "Friends Only." On Instagram, consider making your account **Private**, so that only people you approve can see your photos and posts. This prevents strangers from viewing your content and potentially gathering information about you. Social platforms often default some information to public – take the time to review and adjust those settings. It puts **you** in charge of who sees what.

Be careful about personal information you post: The more personal data you share openly, the easier it is for scammers or identity thieves to use it. For instance, avoid posting things like your full address, phone number, or financial information on your profile or in public posts. Think twice before posting your birth date – if you want to get those Facebook birthday wishes, maybe leave out the year, or keep the post friends-only. Also, **don't overshare your day-to-day whereabouts** publicly. Posting "So excited to be in Hawaii for two weeks!" on a public profile tells everyone that your house might be empty (a potential tip to burglars). It's not that you can't share happy news – just maybe do it in a more controlled way, e.g., share vacation photos after you're back, or share in a private group of friends rather than publicly. Similarly, be cautious about the details in photos. A seemingly innocent picture of you in front of your house could reveal your house number or street sign. Or a photo of your new car might show the license plate. Scammers piecing together info can misuse these details. **Bottom line:** You control what you share – it's okay to share, just do it thoughtfully.

Recognize fake friend requests and profiles: Not everyone on social media is who they claim to be. You might get a friend or follow request from someone with a friendly name or a profile photo of a smiling person – but if you don't actually know them, be cautious. **Only accept friend requests from people you know in real life** or are at least connected to through mutual friends in a verifiable way. A common scam is to receive a friend request from someone you're already friends with. For example, you're already Facebook friends with Jane Doe, but you get a new request from "Jane Doe" with the same picture. That likely means Jane's profile was cloned by a scammer. Decline the new request, and let

your friend know someone is impersonating them. (They may need to report it to Facebook.) If you get a random friend request from a stranger (especially if it's an attractive young person with few other friends or a nearly empty profile), it's probably a fake account. These could be bots or scammers trying to get into your friends list to see your info and possibly message you. **When in doubt, hit "Ignore" or "Delete Request."** It's not rude – it's safe.

Also, be mindful of people who message you out of the blue on these platforms. If you suddenly get a private message from someone you don't know saying "Hi dear, I saw your profile and I have an interesting business proposal" or something along those lines, it's likely a scam or spam. Even if it's from someone you do know (or think you know), be cautious if the conversation quickly turns to requests for money or personal info. Unfortunately, social media accounts can be **hacked**. If a friend's account is compromised, a scammer might message all their contacts with something like "I'm in trouble overseas, can you send money?" – which is basically the Facebook version of the grandparent scam. If you ever get an odd request or message from a friend on social media, call them on the phone to verify. Don't assume it's really them typing to you until you confirm.

Don't overshare personal details in quizzes/games: You've probably seen those cute quizzes like "Your elf name" or "Which 1960s song describes you?" They seem fun, but sometimes they ask for personal info or answers that coincidentally are similar to security questions (e.g., your first car, your mother's maiden name, the street you grew up on). Be wary of those "for fun" posts that ask a bunch of personal questions. Scammers create these to harvest information. It's best to skip those.

Watch out for scam posts and ads: Social media is rife with ads and posts that might not be what they seem. For example, **"limited time offer – get a FREE $100 gift card by clicking here!"**, or sensational news that requires a clickthrough. Many of these are clickbait at best, or malicious at worst. Don't click on links in posts unless you trust the source. Facebook does try to filter out a lot of fake stuff, but it's not perfect. If something appears on your feed with an unbelievable claim or offer, check it through a quick Google search or on Snopes.com (a fact-checking site).

Use strong security on your accounts: This overlaps with the next section (Password & 2FA), but to mention here: *Make sure your social media accounts themselves are secure.* Use a **strong, unique password** for each account so they are less likely to get hacked. And enable **two-factor authentication** on Facebook, Instagram, etc., if available (most have this option in security settings) – that way even if someone guesses your password, they can't get in without the code sent to your phone. This prevents many account takeovers.

Think before you post or comment: Beyond privacy, remember that what you say online can often be seen by more people than you intend. Even if your profile is private, if you comment on a public page (like a news article or company page), that comment is public. Just be mindful – avoid disclosing personal info in public comments or engaging in heated arguments that might attract trolls. Also, assume anything you put online could *eventually* become public, even if you restrict it now (through hacks, policy changes, or someone taking a screenshot).

Social Media Safety Checklist:

- ☐ My social media profiles and posts are set to **private** or **friends-only**, so only people I trust can see my info.
- ☐ I avoid sharing **sensitive details** (address, phone number, financial info) or announcing extended vacations publicly – I share those only with friends, not the whole world.
- ☐ I **only accept friend/follower requests from people I know**. If I get a duplicate request from a friend, I verify with them because it could be a fake. I ignore or report strangers who contact me out of the blue with odd requests.
- ☐ I use a **strong password and 2FA** on my social accounts to prevent hacking (see next section), and I stay alert for any unusual activity on my accounts.