Social Media Safeguards

Welcome to this training lesson on **Social Media Safeguards.** In this lesson, we'll look at ways you can ensure you, your computer or device, and your personal information, remain safe.

Estimated Completion Time: 8 minutes.

Step 1 of 17

Social Media Safeguards

Introduction. Social Media sites - including, but not limited to, FaceBook, Instagram, Twitter, LinkedIn, SnapChat, Google Plus, and others, are incredibly popular ways that people use to communicate with others, share information and photos, and broadcast their point of view.

There are some important guidelines to consider when using Social Media sites to protect your privacy, safety, and reputation.

Social Media Safeguards

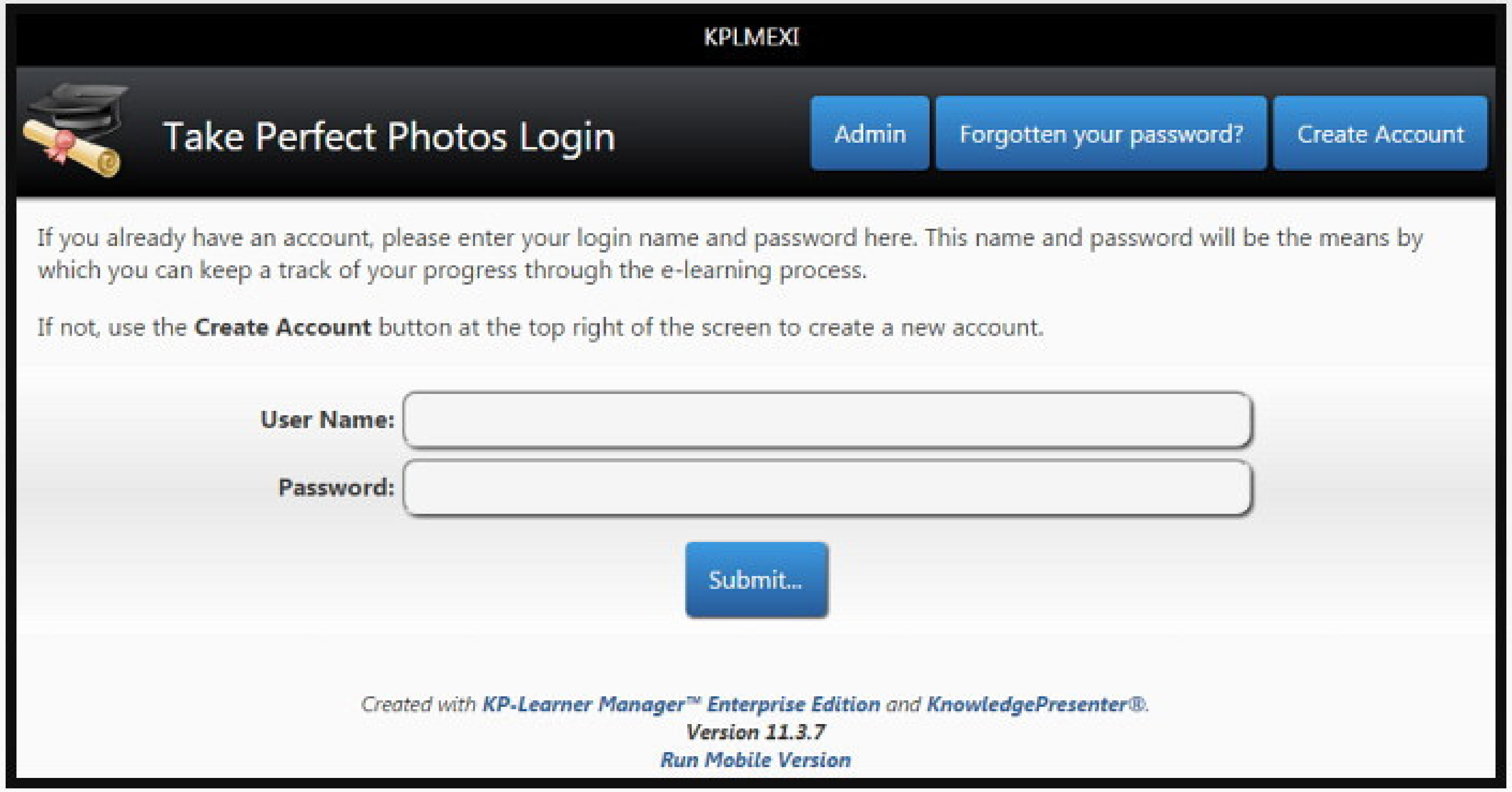
Passwords. Most people use the same password for all their social media - and other - online accounts. This can be a big mistake. As can using a simple password.

Ensure that you look at our **Password Management** lesson. It talks about how you should create, use and manage passwords safely and securely.

Social Media Safeguards

User Names. On most sites, where password access is required, the password is used in combination with a **user name.**

Ensure that you look at our **User Names** lesson. It talks about how you should create, use and manage user names safely and securely.



If you already have an account, please enter your login name and password here. This name and password will be the means by which you can keep a track of your progress through the e-learning process.

If not, use the **Create Account** button at the top right of the screen to create a new account.

User Name:

Password:

Submit...

*Created with **KP-Learner Manager™ Enterprise Edition** and **KnowledgePresenter®**.*
Version 11.3.7
Run Mobile Version

Social Media Safeguards

Sharing Information. The first thing you have to ask yourself - how much information about myself do I want to share?

First of all - what about your most private information? Your address, phone number, date of birth? **Never, ever** share this information online. Even if you *think* you are sharing information privately, that may not be the case. Privacy policies on many social media sites can be confusing.

Social Media Safeguards

What to Share. When posting information online, consider this - don't share anything you don't want the whole world to know. Also, assume it will be online forever.

This applies even for social sites you consider marked as private. You may be hacked, or your followers or friends may be hacked. There are any number of circumstances where your private posts could become public.

Social Media Safeguards

Identity Theft. The more personal information you share online, the easier it will be for hackers - or a stalker - to learn more about you.

The more a hacker knows about you, the easier such things as identity theft and hacking your online accounts will be.

The more a stalker knows about you does not bear thinking about.

Social Media Safeguards

The Innocence of Youth. For younger users, social media sites hold an even greater risk.

Young people don't realise how, *potentially*, social media posts may affect their future life. Organizations, or potential employers, or other contacts may have access to your social media posts going back several years.

A racist or sexist comment, an unfortunate photo, bragging about illegal activities, or disparaging comments about others **must be avoided at all costs.** No potential employer is going to be happy to see such posts. And not even deleting these posts from your account will guarantee they disappear forever.

Social Media Safeguards

Requests for Details. If you are online chatting with, or otherwise communicating with someone you have never met, be very careful. **Never** give out personal information, even when asked. **Never** agree to meet someone you have never met.

The person you are talking to may not be the person you think you are talking to at all.

Social Media Safeguards

Fake Accounts, Followers, and Friends. If you get a friend request from a stranger, keep in mind that hackers and depraved individuals can and will create fake profiles in an attempt to gain your trust. Fake details, fake photos, fake posts are all common.

If you have never met a person, and have no idea who they are, treat them with suspicion. Never divulge personal information - and remember that a follower or friend of your personal site can take information from your profile and use it for nefarious purposes.

Social Media Safeguards

Sexting. Sexting refers to the sending, receiving, or forwarding of images with nudity, sexual, or obscene content. This includes by email, text messages, social media, or apps.

Once again, youth are in most danger of sexting. Peer pressure, lack of awareness of legal ramifications, and responding to requests for 'nude pictures' can lead young people to send, receive or forward such images without any real understanding of the consequences.

And consequences there are. We cover these more in the **Snapchat and Sexting** lesson.

Social Media Safeguards

Cyberbullying. Cyberbullying is the bullying of people using social media sites, either directly to that person, or about that person to other users.

Racist, sexist, or bigoted comments, hate filled comments, or generally disparaging or embarrassing comments may not only be illegal, but can have devastating psychological results for the victim. More than once, young people have committed suicide because of online bullying.

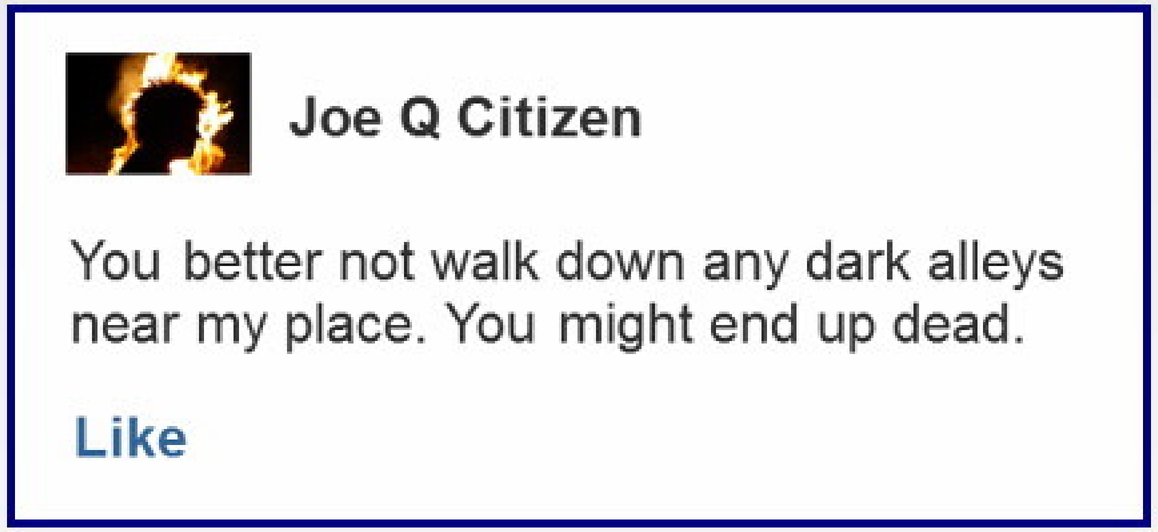
And they **never** reflect well on the people making, forwarding, or 'liking' such comments.

We cover cyberbullying in more detail in the **Cyberbullying** lesson.

Social Media Safeguards

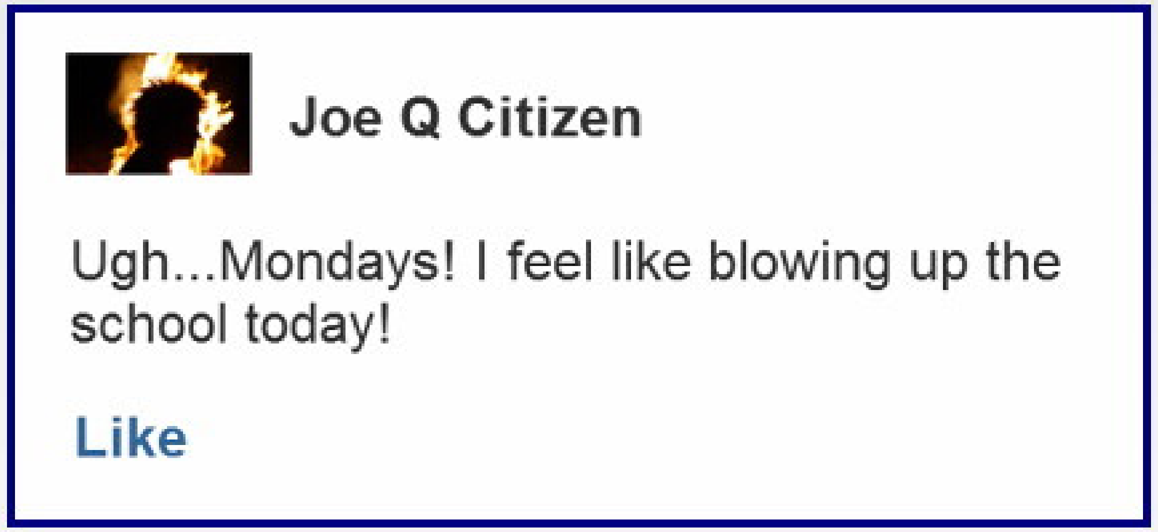
Making Threats. Making threats online - even if you consider it just a joke - is **completely unacceptable.**

Quite apart from possibly alarming people - it is quite possible there are legal ramifications - there are people right now in jail because of threatening posts made in jest.



Joe Q Citizen

You better not walk down any dark alleys near my place. You might end up dead.



Joe Q Citizen

Ugh...Mondays! I feel like blowing up the school today!

Cyberbullying, harrassment, stalking, and/or making threats online could **get your account suspended or cancelled, lose you your job, your education, your career,** and could even **land you in jail. Don't do it.**

Social Media Safeguards

You are Never Anonymous Online. Don't think that because you have created an anonymous account on some social media site, that you cannot be tracked.

Law enforcement has many tools at their disposal should the need be required to track the owner of a particular social media account.

So **don't think** that anonymous accounts will allow you to post threats, or sexual images, or cyberbully without facing the consequences.

Social Media Safeguards

Public Computers. Finally, don't log into social networking sites on shared computers, friends computers, work computers, and in Internet cafes.

Firstly, you don't know what sort of software is installed on those computers that could capture your account details.

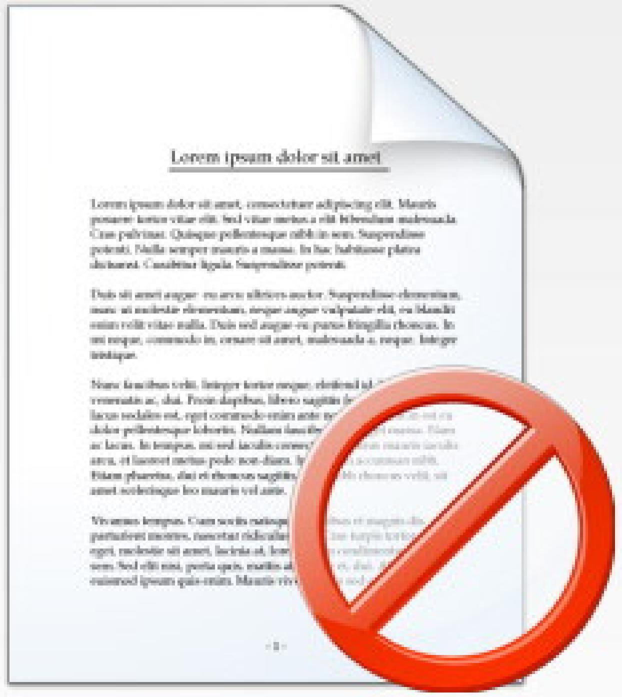
Secondly, if you forget to log out before leaving the computer, you will leave your account wide open to being hacked.

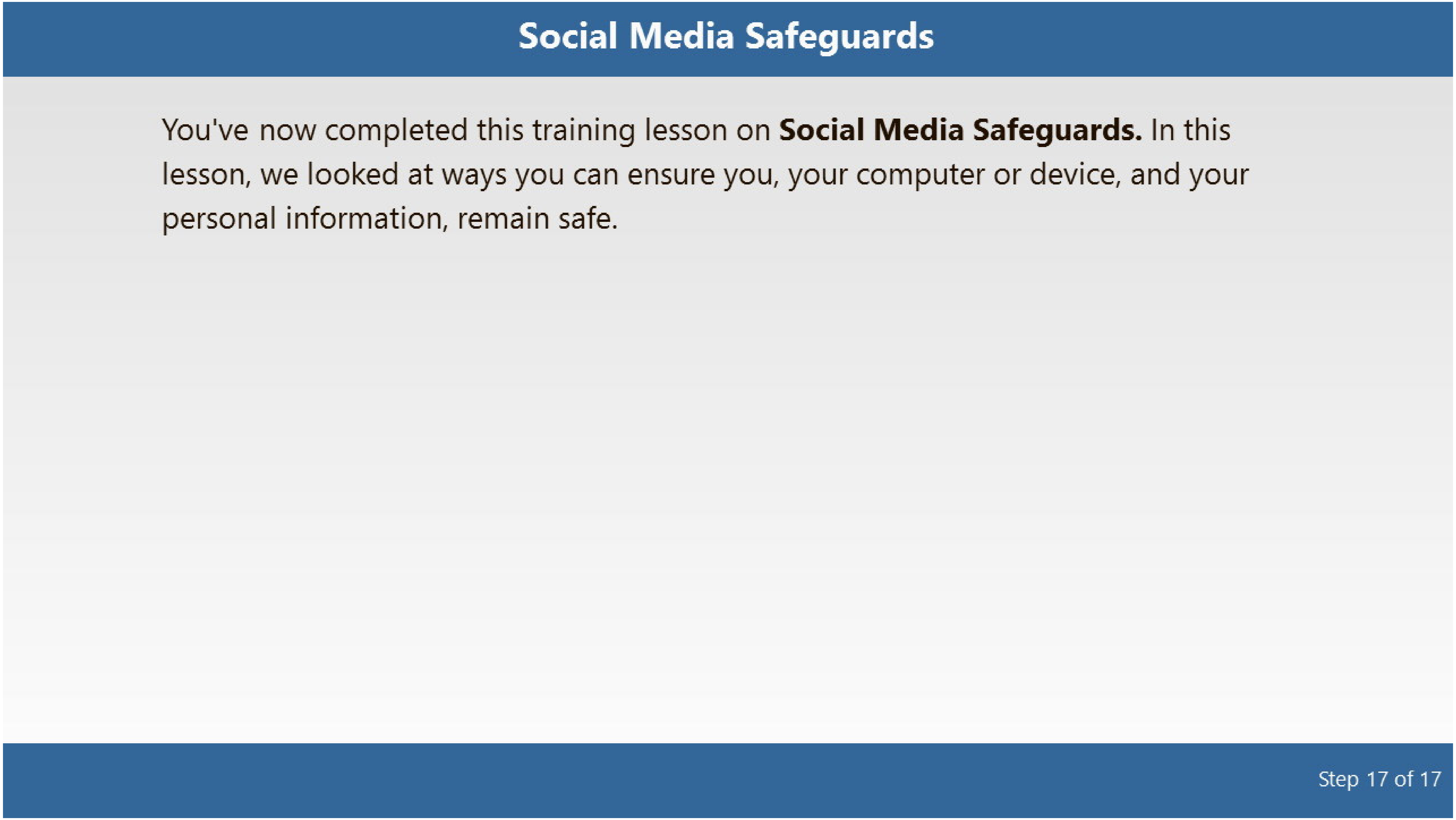
Social Media Safeguards

Friends Computers. If you are under 25, you no doubt seen a friends Facebook page when another 'friend' has posted a comment, pretending to be that person. This can happen when they grab a friends phone, or see that person has not logged out of Facebook on their PC, or some other similar situation.

The fact is that this sort of behaviour is immature, often very embarrassing for the victim, and says little about your character.

Don't do it.





Social Media Safeguards

You've now completed this training lesson on **Social Media Safeguards.** In this lesson, we looked at ways you can ensure you, your computer or device, and your personal information, remain safe.