

ALEXANDRA DIMA

ID: 2323541

GROUP 2

MODULE NAME: DIGITAL SKILLS

MODULE CODE: LCLM4002

INTERNET SAFETY

**DON'T SHARE YOUR
PERSONAL INFORMATION**



NEVER SHARE YOUR PASSWORDS

Strong Passwords



Change your
passwords regularly



Don't share
passwords



Make passwords
hard to guess

**DON'T MEET UP WITH SOMEONE
YOU HAVE MET ONLINE**

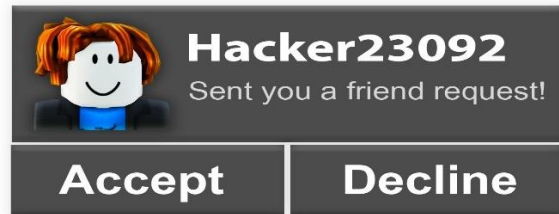


**REPORT INAPPROPRIATE CONTENT
IMMEDIATELY**



**SET UP YOUR DEVICE TO
PROTECT YOUR INFORMATION**

**ONLY ACCEPT FRIENDS REQUEST FROM
PEOPLE YOU KNOW PERSONALLY**



DON'T SHARE YOUR PERSONAL INFORMATION

Give it some thought before sharing information via emails or making any internet posts. Anyone can see what you post online. Online, one of the biggest risks you face is disclosing personal information to people you do not directly know. Think about taking your name off of websites that provide to anyone on the internet any personal information that has been gleaned from public data, such as your address, phone number, and images from social media accounts.

NEVER SHARE YOUR PASSWORDS

When you divulge your password to someone else, you are effectively giving them access to all of your accounts that share that password. Sharing passwords can have the unintended consequence of making your account far less secure right away.

DON'T MEET UP WITH SOMEONE YOU HAVE MET ONLINE

Be cautious about anyone you trust on the internet. Regardless of how long or how friendly you have been conversing with someone you met online, they are still strangers. It can be risky to meet up with these people, therefore only do so with your parents' or carers' consent and only then when they are able to be there.

REPORT INAPPROPRIATE CONTENT IMMEDIATELY

While certain online areas are restricted to adults, others welcome kids. There are Terms of Service or similar documents that specify what can and cannot be shared, regardless of the website, platform, or app.

Social networking sites that permit users who are at least 13 years old will specify in their Terms of Service exactly what kinds of content are prohibited. These most frequently involve violence and nudity.

SET UP YOUR DEVICE TO PROTECT YOUR INFORMATION

Using strong passwords

Install security software on your laptop or computers

Protect your wireless networks

ONLY ACCEPT FRIENDS REQUEST FROM PEOPLE YOU KNOW PERSONALLY

These are four reasons why accepting strange friend requests is not a good idea.

1, people research persons by sending fictitious friend requests. These might be a jealous person who want to hurt you, divorce attorneys, or private investigators.

2, it's possible that the person requesting a friend is a stalker who wants to know more about your tastes and routines.

3, the person who sent the friend request could be a spy with a penchant for corporate espionage

4, it's possible that the requestor is a spammer who is only trying to bother you with advertisements.

References:

[Risk of Sharing Passwords | 4 Reasons Why Sharing Passwords is Bad \(topcontent.com\)](https://topcontent.com/4-reasons-why-sharing-passwords-is-bad/)

[How to avoid sharing too much information online - Get Cyber Safe](#)

[Report Harmful Content - UK Safer Internet Centre](#) [Report Harmful Content - UK Safer Internet Centre](#) [Report Harmful Content - UK Safer Internet Centre](#)