

ONLINE SAFETY

1. **KNOW THE SCAMS; SHARE WHAT YOU KNOW WITH YOUR FRIENDS AND LEARN ABOUT THE DIFFERENT SCAMS AND HOW TO AVOID THEM.**
2. **THINK BEFORE YOU CLICK; DON'T CLICK ON LINKS OR MESSAGES FROM PEOPLE YOU DON'T KNOW AS THIS COULD LEAD TO THEFT OF PERSONAL INFORMATION OR VIRUS DOWNLOADS.**
3. **SAFELY PERUSE, BEWARE OF PHONY WEBSITES. IF A SITE ASKS FOR PERSONAL INFORMATION, THAT YOU DOUBLE CHECK THE URL AND MAKE SURE IT'S NOT ASKING FOR INFORMATION IT SHOULDN'T.**
4. **SHOP SAFELY; YOU SHOULD USE A CREDIT CARD RATHER THAN A DEBIT CARD WHEN SHOPPING ONLINE AS CREDIT CARD COMPANIES ARE MORE WILLING TO REIMBURSE YOU FOR ANY FRAUDULENT CHARGES.**
5. **GOOD PASSWORDS, DON'T USE SIMPLE PASSWORDS LIKE MONKEY123, BECAUSE IT'S VERY EASY TO GUESS. AND DON'T USE SAME PASSWORD FOR CRITICAL ACCOUNTS.**
6. **WATCH YOUR WI-FI CONNECTIVITY. PROTECT YOUR NETWORK BY CHANGING YOUR ROUTER'S DEFAULT SETTINGS AND MAKING SURE YOU HAVE THE CONNECTION PASSWORD-PROTECTED.**
7. **PROTECT YOUR INFORMATION; MAKE SURE TO BACKUP ALL OF YOUR DATA ON YOUR DEVICES IN CASE OF THEFT OR LOSS.**
8. **INSTALL FIREWALL AND ANTIVIRUS SOFTWARE SUCH AS AVAST AND MALWARE, MOST OF YOUR DEVICES WILL COME WITH A FIREWALL BUT THESE AREN'T VERY GOOD AND MOST CYBER ATTACKS WILL GET THROUGH THEM.**
9. **KEEP YOUR SECURITY SOFTWARE UP TO DATE; USE YOUR MANUFACTURER'S LATEST SOFTWARE UPDATE AND MAKE SURE THAT IT AUTOMATICALLY DOES ROUTINE SCANS TO PROTECT YOUR DEVICES.**

SOURCES:

[HTTPS://SECURINGTOMORROW.MCAFEE.COM/CONSUMER/10-TIPS-STAY-SAFE-SURFING-WEB/](https://securingtomorrow.mcafee.com/consumer/10-tips-stay-safe-surfing-web/)

The European Commission accepts no responsibility for the contents of the publication.

Funded by the
Erasmus+ Programme
of the European Union

