How do seniors create safe digital content on social media?

Presented by Samet Mehmet ÇETİN

2024-1-SK01-KA121-ADU-000204079

Slovenský inštitút mládeže IUVENTA

NIVAM
NÁRODNÝ INŠTITÚT VZDELÁVANIA A MLÁDEŽE

Co-funded by the European Union

Nowadays, social media has become a part of the daily life of people of all ages.

Seniors are also increasingly interested in being active on social media.

Co-funded by
the European Union

Attention to Privacy

"Protecting security and privacy is of great importance when creating digital content.

Sensitive data such as phone numbers, addresses and financial information should not be shared."

Secure Password Usage

"Using a secure password is one of the first steps to ensuring digital security.

Passwords need to be strong and complex."

Co-funded by the European Union

SECURE CONNECTIONS

“One should only stay in touch with trusted friends and family members.."

Be careful about messages coming from people you don't know.

Malware

"You should be careful about malware and scam and not click on unknown links.

Co-funded by the European Union

Avoiding Misinformation

Spreading fake news and misinformation should be avoided.

privacy settings

"Privacy settings of social media platforms should be checked regularly."

Co-funded by the European Union

Location and Fraud

Elderly individuals may share location unknowingly while using social media. This can increase the risk of burglars breaking into their home, especially when they are traveling or away from home.

THE IMPORTANCE OF PRIVACY

Seniors may have difficulty understanding privacy settings on social media platforms. This may result in personal information being shared with unwanted people. It is very important to pay attention to privacy settings.

CYBER CRIMES EXPOSED TO ADULTS

In 2022, $3.1 billion in cybercrime damage was reported to the FBI by people over theWhile this figure represents an 82 percent increase over the previous year, there are many more cases that have gone unreported. age of 60 as a result of 88,262 incidents..

PHISHING

A phishing email, phone call or social media message arrives unsolicited. The scammer impersonates a legitimate organization and requests that you provide information such as account logins or click on a link or open an attachment. The former could allow them to take over your accounts, while the latter could result in downloading malware designed to steal more data or crash your computer.

Co-funded by the European Union

ROMANTIC SCAMS

The FBI says romance scams earned scammers $734 billion in 2022. Scammers create fake profiles on dating sites, befriend single and adult individual and establish a rapport with them in order to extrac as much money as possible. Their typical story is that they need money for medical bills or to travel t see their significant other.

Co-funded by the European Union

CARE/HEALTH SERVICES

The scammer impersonates a “Medical Care” representative to obtain personal and medical information that can be sold to others to commit health insurance fraud. They can do this via email, over the phone or even face to face

Co-funded by
the European Union

LOTTERY SCAM

A scammer calls you for no reson and claims that you won the lottery and all you have to do to get your winnings back is to pay a small processing fee or tax up front. Of course, there is no reward and your money will disappear.

Co-funded by
the European Union

Technical Support

One of the oldest phone-based scams is when the scammer impersonates a legitimate organization, such as a technology company or telecommunications provider, to tell you there's something wrong with your computer. This may happen suddenly, or you may be prompted to call a “hotline” after a harmless but alarming pop-up appears on your computer. The scammer may trick you into accessing the machine. They try to find a way to make money from you. It may do this by saying that the machine needs unnecessary “protection” or “upgrading” or by stealing financial information from the machine.

Co-funded by
the European Union

imitation of government

In this case, the scammer pretends to be calling from the Internal Revenue Service, Medical Health Services, or another government agency to request unpaid taxes or other payments. They aggressively warn that failure to pay could lead to arrest or other penalties.

Co-funded by
the European Union

INVESTMENT scam

This category, where cybercriminals earned the highest income by earning more than $3.3 billion in 2022, generally refers to get-rich-quick schemes that promise low risk and guaranteed returns through cryptocurrency investments. In reality, the entire plan is built on sand.

Co-funded by
the European Union

GRANDPARENT SCAM

A scammer calls you unannounced, pretending to be a relative in danger. Usually “Hello grandma, do you know who this is?” They start by saying something like and then follow up with a painful story designed to persuade you to send cash to help them. They usually request payment via money transfer or a cash app. They may ask you to keep everything secret. In some variations on this theme, the scammer poses as a police officer, doctor, or lawyer trying to help your grandchild. Advances in artificial intelligence software known as deepfakes could even enable them to more accurately imitate your grandchild's voice and carry out what's called a "virtual kidnapping scam."

Co-funded by the European Union

HOW TO STAY SAFE

If an offer seems too good to be true, it usually isn't.

Be suspicious of any unsolicited communication. If you want to respond, never reply directly to a message. Instead, Google the sending organization and call or email separately to confirm. Stay calm, do not give your personal information.

Co-funded by the European Union

HOW TO STAY SAFE

Do not trust Caller ID as it may be spoofed. Use multi-factor authentication on your accounts to reduce the threat of someone stealing your login information.

Never send money via wire transfer, payment apps, gift cards or cryptocurrency because there is no way to claim it back in case of scam.

Do not click on links or open attachments in emails, texts, or social media messages.

Co-funded by the European Union

THANKS FOR YOUR ATTENTION

Co-funded by the European Union