EUROPOL

ID THEFT
DO's & DON'Ts

TIPS & ADVICE TO PREVENT IDENTITY THEFT HAPPENING TO YOU

IDENTITY THEFT IS BIG BUSINESS. PERSONAL AND FINANCIAL DATA STOLEN ONLINE IS SOLD IN THE UNDERGROUND ECONOMY, AND IS MISUSED BY CRIMINAL ORGANISATIONS ALL OVER THE WORLD. PROTECTING YOUR DATA DOESN'T JUST SAVE YOU THE INCONVENIENCE OF HAVING TO CHANGE YOUR PASSWORDS AND CREDIT CARDS. IT ALSO HELPS IN THE FIGHT AGAINST ORGANISED CRIME AND TERRORISM.

TO MARK EUROPEAN DATA PROTECTION DAY, EUROPOL'S OPERATIONS DEPARTMENT AND DATA PROTECTION OFFICE HAVE LAUNCHED A JOINT INITIATIVE ON CYBER CRIME & DATA PROTECTION. ON THE RIGHT, EXPERTS FROM THE EUROPOL CYBER CRIME CENTRE SHARE SOME TIPS FOR PREVENTING IDENTITY THEFT.

DON'T:

CLICK ON ATTACHMENTS AND LINKS WITHOUT KNOWING THEIR TRUE ORIGIN. What looks like a harmless video or image can actually be malicious software designed to steal your data. Even opening a spam email can put your address on a spammer's hit list for the future.

GIVE AWAY MORE INFORMATION THAN IS NECESSARY. Your bank and credit card provider already know your pin number and address. They don't need you to tell them via email, phone or web page.

ACCESS ONLINE BANKING FROM SHARED OR PUBLIC COMPUTERS. You never know what might be lurking on its hard drive.

SHARE PASSWORDS, EMAIL ACCOUNTS, OR ANY OTHER ONLINE PERSONAL DATA WITH OTHER PEOPLE. It's so much harder to protect when more than one person has access.

SAVE CREDENTIALS IN BROWSERS. Would you store your password on a sticky note? Saving them in a browser is just as dangerous.

TAKE ANYTHING FOR GRANTED. If an offer in an email or on social media sounds too good to be true, it probably is. It's also really easy for criminals to fake company logos and the identity of senders.

DO:

BE AWARE. Treat unsolicited emails or pages asking for personal information with suspicion, particularly those claiming to be from banks and credit card companies. A quick web search can tell you if the email you've received is a known scam. Remember that you can always check with your bank or credit card company if you receive an email claiming to be from them.

UPDATE YOUR SOFTWARE REGULARLY. Many malware infections are the result of criminals exploiting bugs in software (web browsers, operating systems, common tools, etc.). Keeping these up to date can help to keep you safe.

USE ANTI-VIRUS SOFTWARE. Anti-virus software can help keep your computer free of the most common malware; there are even many free options. Always check downloaded files with AV software. Do not install programs or applications on your computer if you don't know where they have come from.

RESTRICT ACCESS TO YOUR PERSONAL DETAILS ON SOCIAL MEDIA. The more information criminals have access to, the more effectively they can target you. Limiting the amount you share and to whom makes their job harder.

ALWAYS USE STRONG PASSWORDS. Computers can crack most common passwords very quickly. Making sure that your password is strong (above 8 characters and using numbers, letters and symbols) can help.

REPORT IT. If you are a victim of ID theft, report it immediately to your local police and the company affected (bank, online service, etc.). *Law enforcement agencies throughout the EU and around the world work together to disrupt the activities of identity fraudsters and bring scammers to justice. The more information you give to the authorities, the more effectively they can target the most dangerous criminal organisations.*

PO BOX 90850; 2509 LW THE HAGUE; THE NETHERLANDS; PHONE: +31 70 302 5000; E-MAIL: DPO@EUROPOL.EUROPA.EU