SAFE

INTERNET

USE

eTwinning

MEDIA LITERACY
FOR STUDENTS

1. . KEEP PERSONAL INFORMATİON PROFESSİONAL AND LİMİTED

POTENTİAL EMPLOYERS OR CUSTOMERS DON'T NEED TO KNOW YOUR PERSONAL RELATİONSHİP STATUS OR YOUR HOME ADDRESS. THEY DO NEED TO KNOW ABOUT YOUR EXPERTİSE AND PROFESSİONAL BACKGROUND, AND HOW TO GET İN TOUCH WİTH YOU. YOU WOULDN'T HAND PURELY PERSONAL İNFORMATİON OUT TO STRANGERS İNDİVİDUALLY—DON'T HAND İT OUT TO MİLLİONS OF PEOPLE ONLİNE.

2. . *KEEP YOUR PRİVACY SETTİNGS ON*

MARKETERS LOVE TO KNOW ALL ABOUT YOU, AND SO DO HACKERS. BOTH CAN LEARN A LOT FROM YOUR BROWSİNG AND SOCİAL MEDİA USAGE. BUT YOU CAN TAKE CHARGE OF YOUR İNFORMATİON. AS NOTED BY LİFEHACKER, BOTH WEB BROWSERS AND MOBİLE OPERATİNG SYSTEMS HAVE SETTİNGS AVAİLABLE TO PROTECT YOUR PRİVACY ONLİNE. MAJOR WEBSİTES LİKE FACEBOOK ALSO HAVE PRİVACY-ENHANCİNG SETTİNGS AVAİLABLE. THESE SETTİNGS ARE SOMETİMES (DELİBERATELY) HARD TO FİND BECAUSE COMPANİES WANT YOUR PERSONAL İNFORMATİON FOR İTS MARKETİNG VALUE. MAKE SURE YOU HAVE ENABLED THESE PRİVACY SAFEGUARDS, AND KEEP THEM ENABLED.

3. .PRACTİCE SAFE BROWSİNG

YOU WOULDN'T CHOOSE TO WALK THROUGH A DANGEROUS NEİGHBORHOOD—DON'T VİSİT DANGEROUS NEİGHBORHOODS ONLİNE. CYBERCRİMİNALS USE LURİD CONTENT AS BAİT. THEY KNOW PEOPLE ARE SOMETİMES TEMPTED BY DUBİOUS CONTENT AND MAY LET THEİR GUARD DOWN WHEN SEARCHİNG FOR İT. THE INTERNET'S DEMİMONDE İS FİLLED WİTH HARD-TO-SEE PİTFALLS, WHERE ONE CARELESS CLİCK COULD EXPOSE PERSONAL DATA OR İNFECT YOUR DEVİCE WİTH MALWARE. BY RESİSTİNG THE URGE, YOU DON'T EVEN GİVE THE HACKERS A CHANCE.
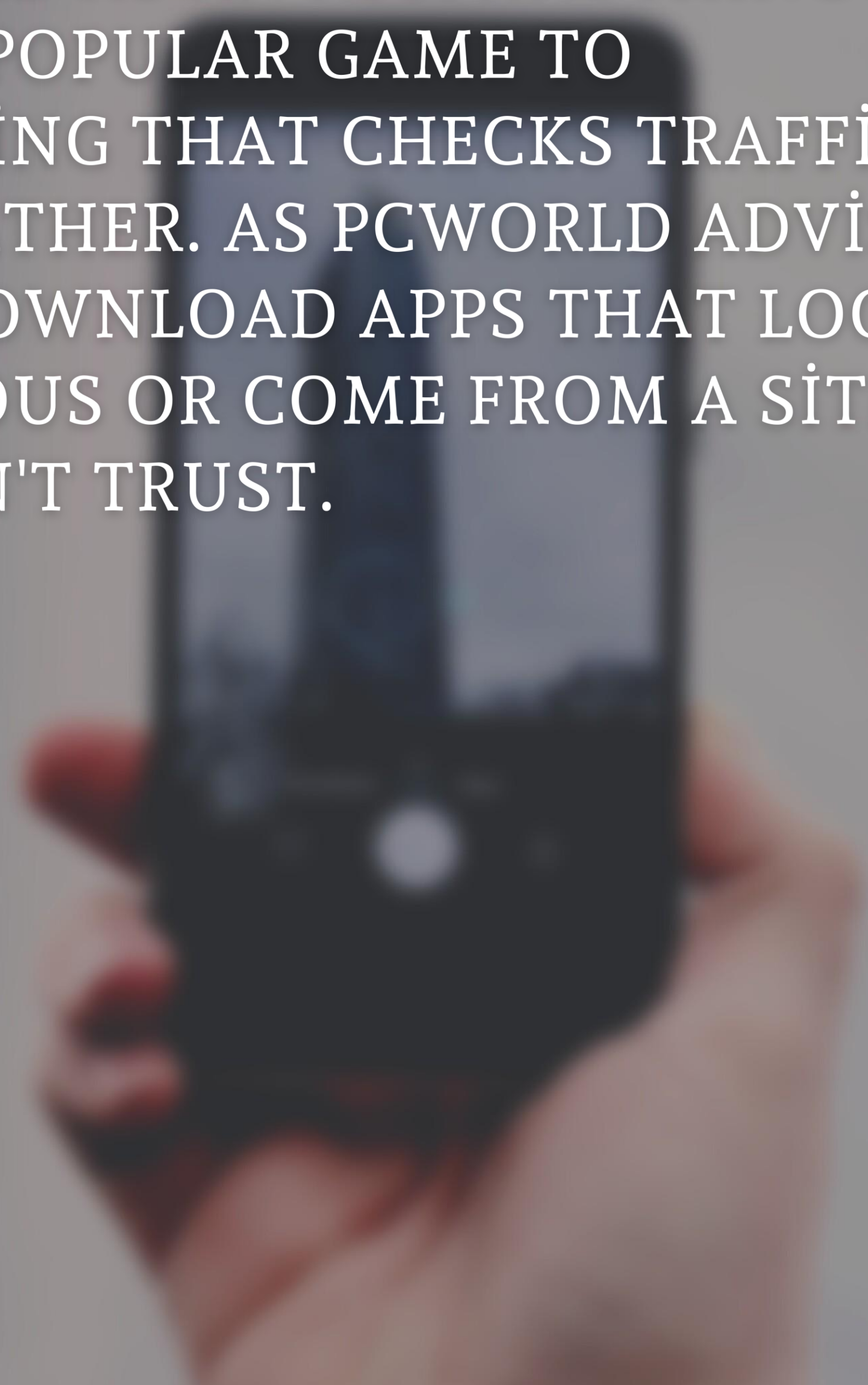
4 . MAKE SURE YOUR INTERNET CONNECTİON İS SECURE. USE A SECUREVPN CONNECTİON

WHEN YOU GO ONLİNE İN A PUBLİC PLACE, FOR EXAMPLE BY USİNG A PUBLİC Wİ-Fİ CONNECTİON, PCMAG NOTES YOU HAVE NO DİRECT CONTROL OVER İTS SECURİTY. CORPORATE CYBERSECURİTY EXPERTS WORRY ABOUT "ENDPOİNTS"—THE PLACES WHERE A PRİVATE NETWORK CONNECTS TO THE OUTSİDE WORLD. YOUR VULNERABLE ENDPOİNT İS YOUR LOCAL INTERNET CONNECTİON. MAKE SURE YOUR DEVİCE İS SECURE, AND WHEN İN DOUBT, WAİT FOR A BETTER TİME (İ.E., UNTİL YOU'RE ABLE TO CONNECT TO A SECURE Wİ-Fİ NETWORK) BEFORE PROVİDİNG İNFORMATİON SUCH AS YOUR BANK ACCOUNT NUMBER.
TO FURTHER İMPROVE YOUR INTERNET BROWSİNG SAFETY, USE SECURE VPN CONNECTİON (VİRTUAL PRİVATE NETWORK). VPN ENABLES YOU TO HAVE A SECURE CONNECTİON BETWEEN YOUR DEVİCE AND AN INTERNET SERVER THAT NO ONE CAN MONİTOR OR ACCESS THE DATA THAT YOU'RE EXCHANGİNG

5. .BE CAREFUL WHAT YOU DOWNLOAD

A TOP GOAL OF CYBERCRİMİNALS İS TO TRİCK YOU İNTO DOWNLOADİNG MALWARE—PROGRAMS OR APPS THAT CARRY MALWARE OR TRY TO STEAL İNFORMATİON. THİS MALWARE CAN BE DİSGUİSED AS AN APP: ANYTHİNG FROM A POPULAR GAME TO SOMETHİNG THAT CHECKS TRAFFİC OR THE WEATHER. AS PCWORLD ADVİSES, DON'T DOWNLOAD APPS THAT LOOK SUSPİCİOUS OR COME FROM A SİTE YOU DON'T TRUST.

6. . CHOOSE STRONG PASSWORDS

PASSWORDS ARE ONE OF THE BİGGEST WEAK SPOTS İN THE WHOLE INTERNET SECURİTY STRUCTURE, BUT THERE'S CURRENTLY NO WAY AROUND THEM. AND THE PROBLEM WİTH PASSWORDS İS THAT PEOPLE TEND TO CHOOSE EASY ONES TO REMEMBER (SUCH AS "PASSWORD" AND "123456"), WHİCH ARE ALSO EASY FOR CYBER THİEVES TO GUESS. SELECT STRONG PASSWORDS THAT ARE HARDER FOR CYBERCRİMİNALS TO DEMYSTİFY. PASSWORD MANAGER SOFTWARE CAN HELP YOU TO MANAGE MULTİPLE PASSWORDS SO THAT YOU DON'T FORGET THEM. A STRONG PASSWORD İS ONE THAT İS UNİQUE AND COMPLEX— AT LEAST 15 CHARACTERS LONG, MİXİNG LETTERS, NUMBERS AND SPECİAL CHARACTERS.

7. . MAKE ONLİNE PURCHASES FROM SECURE SİTES

ANY TİME YOU MAKE A PURCHASE ONLİNE, YOU NEED TO PROVİDE CREDİT CARD OR BANK ACCOUNT İNFORMATİON—JUST WHAT CYBERCRİMİNALS ARE MOST EAGER TO GET THEİR HANDS ON. ONLY SUPPLY THİS İNFORMATİON TO SİTES THAT PROVİDE SECURE, ENCRYPTED CONNECTİONS. AS BOSTON UNİVERSİTY NOTES, YOU CAN İDENTİFY SECURE SİTES BY LOOKİNG FOR AN ADDRESS THAT STARTS WİTH HTTPS: (THE S STANDS FOR SECURE) RATHER THAN SİMPLY HTTP: THEY MAY ALSO BE MARKED BY A PADLOCK İCON NEXT TO THE ADDRESS BAR.

THE INTERNET DOES NOT HAVE A DELETE KEY, AS THAT YOUNG CANDİDATE İN NEW HAMPSHİRE FOUND OUT. ANY COMMENT OR İMAGE YOU POST ONLİNE MAY STAY ONLİNE FOREVER BECAUSE REMOVİNG THE ORİGİNAL (SAY, FROM TWİTTER) DOES NOT REMOVE ANY COPİES THAT OTHER PEOPLE MADE. THERE İS NO WAY FOR YOU TO "TAKE BACK" A REMARK YOU WİSH YOU HADN'T MADE, OR GET RİD OF THAT EMBARRASSİNG SELFİE YOU TOOK AT A PARTY. DON'T PUT ANYTHİNG ONLİNE THAT YOU WOULDN'T WANT YOUR MOM OR A PROSPECTİVE EMPLOYER TO SEE.

9. . BE CAREFUL WHO YOU MEET ONLİNE

PEOPLE YOU MEET ONLİNE ARE NOT ALWAYS WHO THEY CLAİM TO BE. INDEED, THEY MAY NOT EVEN BE REAL. AS INFOWORLD REPORTS, FAKE SOCİAL MEDİA PROFİLES ARE A POPULAR WAY FOR HACKERS TO COZY UP TO UNWARY WEB USERS AND PİCK THEİR CYBER POCKETS. BE AS CAUTİOUS AND SENSİBLE İN YOUR ONLİNE SOCİAL LİFE AS YOU ARE İN YOUR İN-PERSON SOCİAL LİFE.

10. . KEEP YOUR ANTİVİRUS PROGRAM UP TO DATE

INTERNET SECURİTY SOFTWARE CANNOT PROTECT AGAİNST EVERY THREAT, BUT İT WİLL DETECT AND REMOVE MOST MALWARE—THOUGH YOU SHOULD MAKE SURE İT'S TO DATE. BE SURE TO STAY CURRENT WİTH YOUR OPERATİNG SYSTEM'S UPDATES AND UPDATES TO APPLİCATİONS YOU USE. THEY PROVİDE A VİTAL LAYER OF SECURİTY.

KEEP THESE 10 BASİC INTERNET SAFETY RULES İN MİND AND YOU'LL AVOİD MANY OF THE NASTY SURPRİSES THAT LURK ONLİNE FOR THE CARELESS.

MEDIA LITERACY FOR STUDENTS

İLKNUR AVAŞİN