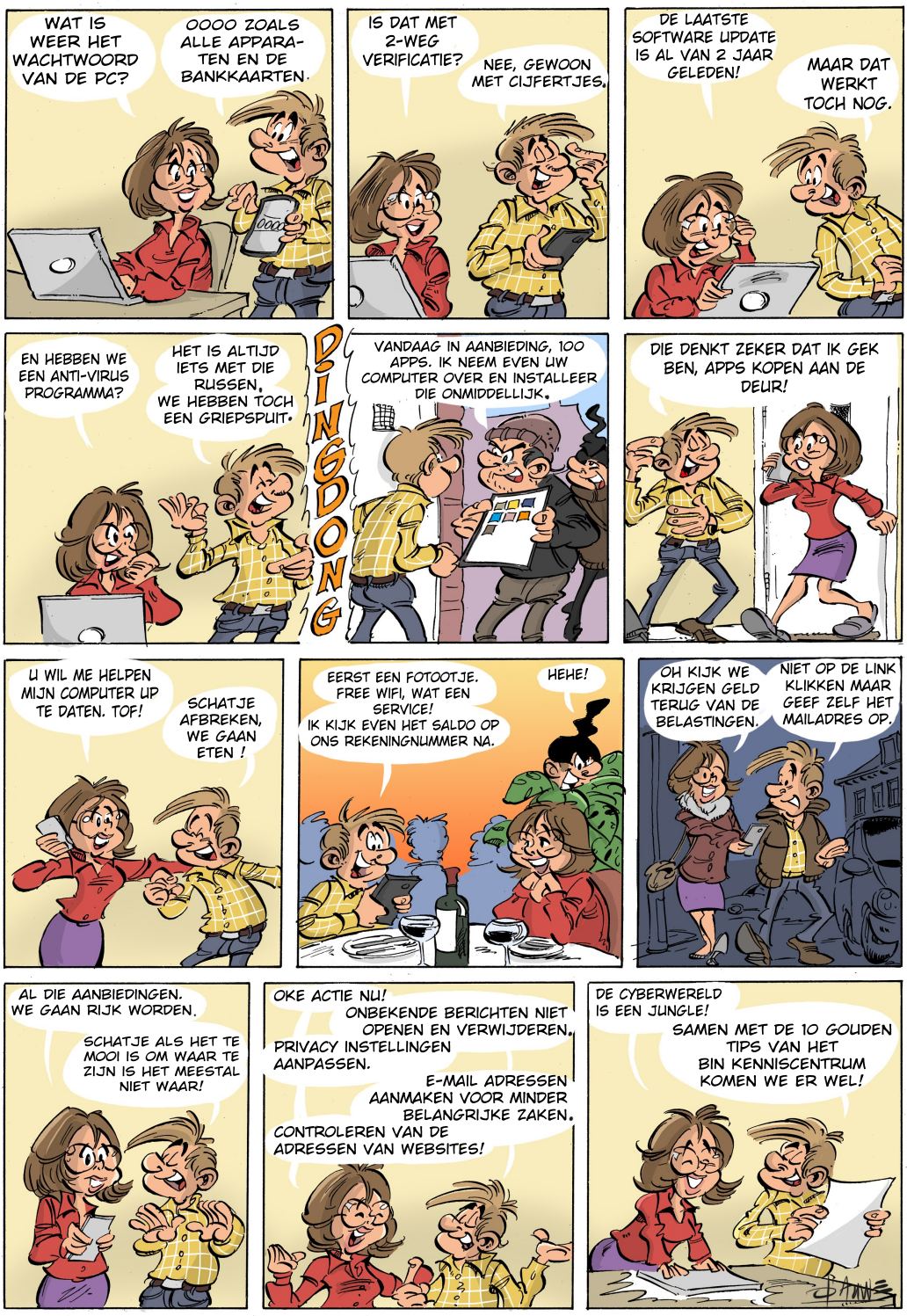
WAT IS WEER HET WACHTWOORD VAN DE PC?
OOOO ZOALS ALLE APPARATEN EN DE BANKKAARTEN.
IS DAT MET 2-WEG VERIFICATIE?
NEE, GEWOON MET CIJFERTJES.
DE LAATSTE SOFTWARE UPDATE IS AL VAN 2 JAAR GELEDEN!
MAAR DAT WERKT TOCH NOG.
EN HEBBEN WE EEN ANTI-VIRUS PROGRAMMA?
HET IS ALTIJD IETS MET DIE RUSSEN. WE HEBBEN TOCH EEN GRIEPSPUIT.
DINGDONG
VANDAAG IN AANBIEDING, 100 APPS. IK NEEM EVEN UW COMPUTER OVER EN INSTALLEER DIE ONMIDDELLIJK.
DIE DENKT ZEKER DAT IK GEK BEN, APPS KOPEN AAN DE DEUR!
U WIL ME HELPEN MIJN COMPUTER UP TE DATEN. TOF!
SCHATJE AFBREKEN, WE GAAN ETEN !
EERST EEN FOTOOTJE. FREE WIFI, WAT EEN SERVICE! IK KIJK EVEN HET SALDO OP ONS REKENINGNUMMER NA.
HEHE!
OH KIJK WE KRIJGEN GELD TERUG VAN DE BELASTINGEN.
NIET OP DE LINK KLIKKEN MAAR GEEF ZELF HET MAILADRES OP.
AL DIE AANBIEDINGEN. WE GAAN RIJK WORDEN.
SCHATJE ALS HET TE MOOI IS OM WAAR TE ZIJN IS HET MEESTAL NIET WAAR!
OKE ACTIE NU! ONBEKENDE BERICHTEN NIET OPENEN EN VERWIJDEREN. PRIVACY INSTELLINGEN AANPASSEN. E-MAIL ADRESSEN AANMAKEN VOOR MINDER BELANGRIJKE ZAKEN. CONTROLEREN VAN DE ADRESSEN VAN WEBSITES!
DE CYBERWERELD IS EEN JUNGLE! SAMEN MET DE 10 GOUDEN TIPS VAN HET BIN KENNISCENTRUM KOMEN WE ER WEL!

o Deze geheugenkaart, in de vorm van een korte strip, helpt je te voorkomen dat je het slachtoffer wordt van cybercriminaliteit.
o Gebruik je gezond verstand! Als iets te mooi lijkt om waar te zijn dan is het dat meestal ook.
o Wees altijd alert en sceptisch als je iets niet vertrouwt.

Maak zeker gebruik van onderstaande tips om veilig op het internet te surfen.

1. Gebruik complexe wachtwoorden en/of lange wachtwoordzinnen. Gebruik nooit hetzelfde wachtwoord voor verschillende toepassingen. Verander regelmatig je wachtwoord. Gebruik een wachtwoordkluis of wachtwoordenboekje als geheugensteun. Leg het boekje steeds op een veilige plaats en niet naast je computer.
2. Kies indien mogelijk voor tweestapsverificatie. Al heel wat bedrijven en instellingen bieden deze mogelijkheid aan.
3. Installeer altijd de officiële software-updates. Zo verklein je de kans dat je gehackt wordt. Maak regelmatig back-ups van je bestanden.
4. Installeer een antivirusprogramma op al je toestellen en niet alleen op je computer/laptop. Schakel automatische updates in voor je antivirusprogramma en je software. Maak ook gebruik van een firewall.
5. Open geen berichten en onbekende bestanden die je niet verwacht of vertrouwt.
6. Installeer alleen apps via de officiële applicatiewinkels (Playstore voor Microsoft, Applestore voor Apple).
7. Controleer het adres van websites op onregelmatigheden. Indien je twijfelt, neem dan contact op via het vertrouwde adres van de instelling of organisatie.
8. Verbreek het contact met ongevraagde helpdeskmedewerkers. Indien je twijfelt, bel dan terug via het officiële telefoonnummer van de instelling of het bedrijf.
9. Stel je privacyinstelling zo hoog mogelijk in op sociale media. Alles wat je plaatst kan ge(mis)bruikt worden.
10. Maak alleen verbinding met vertrouwde wifinetwerken, liefst geen publieke wifinetwerken.

o Het naleven van de preventietips verkleint het risico op cybercriminaliteit.
o Noch de vrijwilliger, noch de organisaties achter deze campagne zijn aansprakelijk indien een burger toch slachtoffer wordt van enige vorm van cybercriminaliteit.

BIN **Kenniscentrum**
Buurt.Informatie.Netwerk

VU : VZW BIN Kenniscentrum – www.bin-plp.be