Transcipt De SeniorWeb Podcast

Zegert van der Linde in gesprek met Peter Rollé

00:00:00

Zegert van der Linde: Welkom bij de SeniorWeb Podcast. Mijn naam is Zegert van der Linde. Fijn dat u luistert.

00:00:05

Zegert van der Linde: De maand maart staat SeniorWeb in het teken van online veiligheid en privacy. In deze vier podcastafleveringen praat ik met verschillende gasten over dit thema. U krijgt achtergronden, verdieping en praktische tips om veilig online te gaan.

00:00:21

Zegert van der Linde: Een rekening betalen, boodschappen doen, boeken aanschaffen, we doen steeds meer financiële transacties online. Dat is makkelijk, maar roept natuurlijk ook vragen op. Want hoe veilig is dat online betalen? Daar ga ik het vandaag over hebben met mijn gast, Peter Rollé van de Rabobank. Welkom Peter.

00:00:43

Peter Rollé: Dank je.

00:00:44

Zegert van der Linde: Inmiddels is online bankieren bijna niet meer weg te denken, maar weet jij nog het moment dat je voor het eerst bij de bank inlogde?

00:00:50

Peter Rollé: Het exacte moment kan ik me niet meer heugen, maar ik weet wel dat toen ik begon met werken bij een bank, ik denk toch wel even twintig jaar geleden, dat het internetbankieren echt een dienst was die nog apart aangeboden werd, naast, we zullen maar zeggen, regulier de acceptgiro en de overschrijvingskaartjes. Ja, dus ik weet wel de opkomst. Dat is, denk ik, een twintig jaar geleden ondertussen.

00:01:14

Zegert van der Linde: Twintig jaar nog maar eigenlijk ook hè, aan de andere kant. Twintig jaar geleden hadden we allemaal nog zo'n map in de... Ik heb nog één zo'n map van vroeger in de kast inderdaad, met allemaal van die afschriften. Elke week eentje.

00:01:25

Peter Rollé: En een boekje overschrijvingskaarten. En op de maandagochtend, als je dan bij de bank begon met werken, gooide je de brievenbus open. En niet overdreven, daar viel echt een stapel overschrijvingskaartjes op de mat en die werden toen verwerkt.

00:01:41

Zegert van der Linde: Dit klinkt voor mij echt als iets uit een ver verleden, maar toch zijn er nog steeds mensen die niet online bankieren, die niet online winkelen, die geld uit de muur halen om te betalen. Hoelang kan dat nog?

00:01:55

Peter Rollé: Ik denk dat er wel een klantengroep bij banken is die dat wil blijven gebruiken, ik wil bijna zeggen, totdat het een beetje een uitgestorven ras is, hè. Dat dat uiteindelijk de ouderen zijn die er niet mee bekend zijn geworden en die het toch prettig vinden om het nog op papier te doen. Het is een stukje dienstverlening wat de komende jaren wel zal blijven. Maar je ziet wel dat zo'n negen op de tien klanten bij de banken online of via de app bankieren. En voor betalen met overschrijvingskaarten worden nu bijvoorbeeld zelfs kosten in rekening gebracht, terwijl het internetbankieren gratis is.

00:02:31

Zegert van der Linde: Maar je zegt dus: mensen die dit nog niet digitaal doen, die niet digitaal bankieren, die zijn er gewoon niet mee bekend geworden. Maar lopen zij niet meer risico?

00:02:41

Peter Rollé: In zekere zin wel. Het is helaas nog zo dat oplichters ook nog steeds de acceptgiro en de overschrijvingskaarten proberen te vissen bij de brievenbussen of bij de postverzending. En het fysieke risico daarbij is natuurlijk groter dan als je gewoon zelf, via een app een betaling doet, als je dat op een veilige manier doet. Dus ja,

als je het hebt over veiligheid... Neem ook contant geld. Als je je broek in de was gooit en er zit nog een biljet in, dan mag je hopen dat hij er goed uitkomt. Maar ik kan me ook nog wel herinneren: vroeger, als je bijvoorbeeld ging stappen en je had contant geld mee en het raakte uit je broekzak of iemand was aan het stelen die avond, dan was het gewoon weg. En dat is toch wat lastiger met de huidige middelen, met toegangscodes, met pincodes, met Touch ID. Dus als je het hebt over veiligheid, kun je bijna wel stellen dat het huidige betalingsverkeer veiliger is dan de fysieke middelen van vroeger.

00:03:37

Zegert van der Linde: Ik moet ik zeggen: die enkele keer dat ik nog veel contant geld op zak heb, dan voel ik me altijd een beetje... Ik heb altijd het idee dat mensen dat op de een of andere manier aan me kunnen zien of zo. Tegenwoordig gaan bijna alle bankzaken -je zei al negen op de tien, misschien over een poosje nog wel meer- digitaal. Het gebeurt allemaal digitaal. Op wat voor manieren zorgen banken ervoor dat dit veilig gebeurt?

00:04:06

Peter Rollé: De voornaamste veiligheid bij banken zit in een stuk authenticatie, dus dat betekent eigenlijk dat je bijvoorbeeld zelf je code kiest om de app te installeren. Daarbij zie je nog altijd het fysieke kastje bij de banken, dat bijvoorbeeld het doen van een betaling via internetbankieren of bijvoorbeeld het installeren van de app nog altijd met een responscode gaat of een code die je krijgt van de bank en op je code-apparaatje intoetst. Dus daar zit gewoon veel veiligheid op. Daarbij is het zo dat de betrouwbaarheid van online bankieren 99,9% is, dus het is ook altijd heel erg beschikbaar. En het is natuurlijk met wat jij noemde, de acceptgiro en overschrijvingskaarten, dat je moet wachten tot hij verwerkt is. En eigenlijk kun je daarvan zeggen: het is niet heel beschikbaar.

00:04:55

Zegert van der Linde: Nee, want nu, als je straks weer op een verjaardagsfeestje zit en je hebt met zijn allen een cadeau gekocht en om tien uur zegt iemand: "O, ja, wil jij nog eventjes het cadeau naar mij betalen?" dan kun je met je telefoon erbij direct het geld overmaken, op zaterdagavond om tien uur.

00:05:07

Peter Rollé: Twee seconden is het er.

00:05:09

Peter Rollé: Ja, inderdaad. Veel banken hebben natuurlijk ook een app, hè. Ik denk dat ze het allemaal wel hebben. Ik heb me weleens laten vertellen dat die app veiliger is dan de website. Klopt dat?

00:05:22

Peter Rollé: In zekere zin wel. Het nadeel van het bezoeken van een website is dat je goed moet checken of je op de juiste website zit. Dus stel: je krijgt een bericht van bijvoorbeeld de Belastingdienst of een energiebedrijf of van de bank zelf en je wordt doorgeleid via de link naar een bepaalde site die eruitziet als de echte site van de bank, dan kan je te maken krijgen met phishing. En phishing is feitelijk alleen maar mogelijk op een internetsite. Phishing via de app is tot op heden nog niet gelukt bij de boeven, hè. Wie weet. Dus in die zin kun je bij een bankieren app altijd veilig bankieren, want hij is geïnstalleerd op je telefoon, het is een stukje software. Daarbij is het zo dat je inlogt met je persoonlijke toegangscode of je Finger ID of Touch ID, net hoe je dat gebruikt, terwijl je bij het internetbankieren dus ook zomaar op bijvoorbeeld www.raboobank, met twee o's terechtkomt. Dus daar moet je altijd extra opletten. Als je het hebt over gewoon het bezoeken van de website, dan zijn beide net zo veilig met de juiste handelwijze van de rekeninghouder.

00:06:36

Zegert van der Linde: Maar het is dus puur dat linkje, hè? In aflevering één heb ik het daar met Esther Mieremet ook al even over gehad. Klik niet zomaar op dat linkje. Ga dan gewoon naar de website van de bank, als dat even kan.

00:06:48

Peter Rollé: Zeker, ja.

00:06:50

Zegert van der Linde: En dan zit je, als je zelf goed het adres intypt, eigenlijk net zo veilig als wanneer je de app op je telefoon pakt?

00:06:55
Peter Rollé: Klopt, ja. Maar wat je ook steeds meer ziet, is natuurlijk dat bedrijven ook gebruik maken van bijvoorbeeld apps. Neem bijvoorbeeld een bol.com. Die hebben een app. Daar heb je op een gegeven moment een factuur klaarstaan en als je dan bijvoorbeeld je factuur gaat betalen, dan word je doorgeleid naar iDEAL en omdat het op je mobiel is, wordt hij doorgeleid naar je mobiele app van de bank. Die route is super veilig, die gaat nooit fout. Als je daarentegen dus een nepfactuur krijgt van bol.com in een e-mail en je gaat dus naar een website, dan dan heb je daar een groter risico. Zeker. Dus het is heel erg belangrijk om die link te checken. En als je het niet helemaal vertrouwt, ga gewoon naar de website toe waar je bijvoorbeeld een factuur van hebt of bel desnoods het bedrijf waar je de factuur van krijgt even op.
00:07:45
Zegert van der Linde: Ja, even checken.
00:07:46
Peter Rollé: Even checken, zeker. En dan ga je ouderwets weer bellen. Dus ja, je kunt eigenlijk zeggen: tegenwoordig is het online bankieren met de app heel gangbaar. Maar het ouderwetse belletje van: "Klopt het dat ik van jullie een rekening krijg?" dat moet je zeker doen.
00:08:00
Zegert van der Linde: Blijft toch altijd goed. Dus het zwakste punt van de app is eigenlijk de gebruiker van de app?
00:08:06
Peter Rollé: Altijd.
00:08:06
Zegert van der Linde: Altijd.
00:08:06
Peter Rollé: Helaas is altijd de conclusie bij elk fraudeonderzoek wat bij de bank plaatsvindt dat toch vaak de gebruiker, de rekeninghouder de zwakste schakel is. Die heeft eigenlijk gegevens achtergelaten op een site die door oplichters wordt meegekeken.
00:08:22
Zegert van der Linde: Dan komen we bij dat online winkelen. We zijn de laatste jaren en misschien zelfs ook wel het laatste jaar nog extra veel online gaan winkelen. Ik bedoel, het aantal bezorgbusjes in de straat is bijna niet meer te tellen. Kan dat dan altijd veilig? Laat ik het zo zeggen: hoe weet je dat zo'n winkel waar jij komt veilig is?
00:08:43
Peter Rollé: Je kunt ervan uitgaan dat als je een aanbod ziet op een site die je nog niet eerder hebt ontdekt... Dus bijvoorbeeld, je googelt op een bepaald product en dan komen er een aantal uit dat je denkt: nou, deze website heb ik nog nooit gezien, ik ga eens even kijken. En het is een aanbod... Ik noem altijd de PlayStation 5.
00:09:04
Zegert van der Linde: Spelcomputer, de nieuwste.
00:09:04
Peter Rollé: De nieuwste spelcomputer. Niet te krijgen. Maar er is een website die hem wel krijgt, ook nog voor een hele mooie prijs, dan weet je eigenlijk zeker: dit klopt niet helemaal. Dus als het te mooi is om waar te zijn, is het te mooi om waar te zijn.
00:09:17
Zegert van der Linde: Ja, dus eigenlijk ook dat is weer net als in het echte leven. Als het te mooi lijkt om waar te zijn, dan is het dat ook meestal ook.
00:09:24
Peter Rollé: Klopt. Dus als je gewoon een betrouwbare website of webwinkel bezoekt, neem bol.com, Coolblue, MediaMarkt, dat soort winkels, kun je er gewoon van uitgaan: dat is goed. Die hebben een goede klantenservice, zijn bereikbaar. Daar is het zo dat als je wel op een website komt en je moet bijvoorbeeld al een betaling doen naar het buitenland of gekke dingen, bijvoorbeeld alleen maar betaling vooraf mogelijk en niet achteraf, dan moet je eigenlijk al gaan nadenken van: wil ik dit wel?

00:09:56
Zegert van der Linde: En bijvoorbeeld Marktplaats, weet jij ook hoe die dat regelen? Want dan is het natuurlijk nog wel een stapje lastiger, omdat je dan wel Marktplaats hebt als betrouwbare partij, maar je weet niet wie er aan de andere kant zit, die jou die -ik noem maar wat- tafel aanbiedt.
00:10:13
Peter Rollé: Klopt.
00:10:13
Zegert van der Linde: Weet jij hoe Marktplaats dat regelt, dat dat veilig gaat?
00:10:17
Peter Rollé: Bij Marktplaats is het eigenlijk zo dat je binnen een seconde of drie een account hebt aangemaakt. Je hebt daar eigenlijk alleen maar een mailadres voor nodig. Dat heb je met tien seconden aangemaakt, zeg ik altijd. Dus de veiligheid op Marktplaats... Je moet ervan uitgaan dat het niet klopt. Als je dat als uitgangspunt neemt en dan ga je een aantal controles doen, zoals bijvoorbeeld: kan ik contact krijgen met die persoon, heeft hij reviews van anderen, heeft hij een langere gebruikershistorie? Waarbij je ook dan in je achterhoofd moet houden dat dat soort accounts ook wel gehackt worden. Dus iemand die bijvoorbeeld vijftien jaar actief is op Marktplaats, maar bijvoorbeeld zijn wachtwoord niet goed heeft beveiligd, daarvan kan er zomaar een oplichter met zijn account bezig zijn. Bij Marktplaats is het heel erg van belang om je af te vragen, bijvoorbeeld wat jij noemt, een tafel, wil je die kopen in Breda of Rotterdam, terwijl je bijvoorbeeld in Groningen woont? Zoek gewoon meer in je regio en probeer gewoon bij iemand aan de deur te komen, ook al is dat lastig in deze coronatijd, begrijp ik, maar ga er gewoon vanuit dat je een beetje in een bepaalde cirkel moet blijven. En als je een keer wel een aankoop doet en je betaalt het vooraf, bestaat de kans dat je wordt opgelicht. En dat risico moet je zelf nemen. Wat bij Marktplaats belangrijk is om te beseffen, is dat er heel veel phishing plaatsvindt via Marktplaats. Dus op het moment dat je nu bijvoorbeeld kijkt naar de e-mailtjes en sms'jes die je soms krijgt van bijvoorbeeld je bank: "U heeft een nieuwe pas, klik hier." De klikkans wordt steeds kleiner, want mensen worden steeds meer bewust van dat soort phishing. Het verplaatst een beetje naar dat soort media als Marktplaats, maar ook bijvoorbeeld Instagram en Facebook. De oplichters creëren een soort vertrouwensband van: "Ik heb een product, wil je het van me kopen? Ik heb hier bijvoorbeeld een PostNL label of DHL label voor je." Of inderdaad een linkje van de bank. In die modus zitten dan oplichters dat er sneller geklikt wordt, want mensen vertrouwen het of die willen iets aankopen. Dus Marktplaats wordt eigenlijk gebruikt voor phishing.
00:12:21
Zegert van der Linde: Het wordt steeds lastiger.
00:12:23
Peter Rollé: Het wordt steeds lastiger.
00:12:23
Zegert van der Linde: Ze worden natuurlijk ook steeds slimmer.
00:12:24
Peter Rollé: Steeds slimmer, ja. Wij zien ook bij de bank steeds meer verschillende manieren dat je denkt: hoe bedenken ze het? Maar ze bedenken het.
00:12:32
Zegert van der Linde: Dus de grondhouding, denk ik, de basis is gewoon: blijf altijd goed opletten. Blijf alert.
00:12:38
Peter Rollé: Zeker.
00:12:39
Zegert van der Linde: Houd het in de gaten.
00:12:41
Zegert van der Linde: Dan iets wat ik zelf altijd nog wel een klein beetje spannend vind, maar ik ben er inmiddels ook al wel achter dat dat een beetje irreëel is: creditcardbetalingen. Ik vind dat op de een of andere manier altijd een beetje

spannend als ik mijn gegevens daar invul en zo. Maar toen hoorde ik laatst: "Maar creditcardbetalingen zijn heel veilig." Klopt dat?

00:13:00

Peter Rollé: Ja, creditcardbetalingen zijn veilig, net zo veilig eigenlijk als betalen bij de bank. Het voordeel daarvan is dat je bij de meeste creditcardmaatschappijen steeds meer de aankoopgarantie hebt. Dus stel: je hebt een webwinkel waarvan je denkt: nou, ik doe een eerste keer een bestelling. Het ziet er allemaal wel goed uit. Ze hebben bijvoorbeeld een label van het thuisbezorg waarborgfonds. Dan kun je met een creditcardbetaling die aankoopgarantie hebben. Dat stel: het pakketje wordt niet geleverd, dan heb je met een creditcard dus een aankoopgarantie. En daarbij zie je ook creditcardmaatschappijen richting de app gaan, waarbij ze bijvoorbeeld de betaling laten verifiëren met de app van bijvoorbeeld de creditcardmaatschappij. Dus waar je ook je betaling moet verifiëren, zie je ook steeds meer creditcardverificatie.

00:13:50

Zegert van der Linde: Ja, misschien is mijn angst ook wel dat ik dan denk: straks komen mijn creditcardgegevens in verkeerde handen. En op een creditcard zit natuurlijk een behoorlijk limiet, daar kun je behoorlijk op een dag mee uitgeven. Dat ik dat spannend vind of zo.

00:14:05

Peter Rollé: Dan kun je je afvragen... Want er is een mogelijkheid om bijvoorbeeld je creditcardgegevens op te slaan bij websites. Dat moet je eigenlijk niet willen, dus maak daar gewoon geen gebruik van. Dan klop je elke keer wel dat zestiencijferige nummer in. Dat is best elke keer even een moeite, maar laat gewoon zo weinig mogelijk informatie achter bij derden. Want als zij bijvoorbeeld een keer gehackt worden of de gegevens komen op straat te liggen, dan ligt ook jouw creditcardnummer op straat en daar moet je voor oppassen.

00:14:36

Zegert van der Linde: Geldt dat... Dat is trouwens sowieso wel een goeie tip: niet dingen opslaan. Dat kan betekenen mijn bankgegevens, je bankrekeningnummer, niet zomaar ergens het vinkje aanzetten: "Bewaar deze gegevens".

00:14:48

Peter Rollé: Klopt. Kijk, op zich een bankrekeningnummer zelf die op straat ligt, dat kan helemaal geen kwaad. Dat is hetzelfde als jij je pinpas verliest en je blokkeert hem direct bij de bank, dan is het een waardeloos ding. Maar met de juiste combinatie van bijvoorbeeld de pincode, CVC code bij de creditcard, persoonlijke gegevens, dat kan benut worden, als dat in verkeerde handen komt.

00:15:11

Zegert van der Linde: We maken ook steeds vaker geld over via apps bijvoorbeeld. Ik krijg nog weleens een Tikkie. Kun jij heel kort even uitleggen: wat is een Tikkie?

00:15:20

Peter Rollé: Nou, Tikkie is een middel, een aparte app van ABN AMRO Bank, terwijl ING en Rabobank binnen de bankieren app een betaalverzoek hebben. En ABN AMRO Bank heeft als het ware een dochterbedrijf gecreëerd, dat is dan Tikkie en dat is dan weer te gebruiken voor alle Nederlandse banken. Waar Tikkie op neerkomt, is een iDEAL betaling, dus je creëert eigenlijk een iDEAL link die je naar iemand toestuurt en op het moment dat die de betaling doet, wordt die doorgeleid naar een iDEAL omgeving en doet de betaling.

00:15:53

Zegert van der Linde: En iDEAL is dus dat wat je kent van -wij noemden ze al- bol.com bijvoorbeeld, als je daar met je bankrekening je bestelling betaalt. Dat is ook een iDEAL betaling. Dat is eigenlijk hetzelfde. Dus dat is dat.

00:16:02

Peter Rollé: En je kunt tegenwoordig ook via een Tikkie app en ook de betaalverzoekapps van de andere banken QR-codes aanmaken. Ook dat is weer een snelle manier van een betaling doen. Hoef je niet eens een linkje naar iemand toe te sturen. Je laat de QR-code zien op je telefoon en iemand kan via de link betalen. Ook bij collectes aan de deur bijvoorbeeld, dan zie je uniforme QR-codes. Dus als er dan collectes zijn en je hebt vandaag de dag minder contant in huis, dan kun je dus via de QR-codes de collectebus vullen.

00:16:33
Zegert van der Linde: Ideaal.
00:16:33
Peter Rollé: Ideaal. Geen rammelende munten meer.
00:16:38
Zegert van der Linde: Nee, geen zware collectebus meer voor de collectant en ik hoef geen geld meer in huis te hebben. Je zegt wel iets interessants. Tikkie is een losse app van ABN AMRO. Rabobank en ING bieden het aan als betaalverzoek vanuit de apps, zo ken ik het ook. Zit er nog een verschil in veiligheid tussen de twee?
00:16:56
Peter Rollé: Nee, het is allemaal veilig. Het enige waar je op moet letten, is dus als je een Tikkie of een betaalverzoek krijgt: klopt het dat ik dat betaalverzoek krijg? Klopt het bedrag? Je ziet bijvoorbeeld oplichting met WhatsApp, dus iemand krijgt een app van bijvoorbeeld zijn zoon of dochter.
00:17:12
Zegert van der Linde: Tussen aanhalingstekens.
00:17:12
Peter Rollé: Tussen aanhalingstekens, ja. Het is niet de echte zoon of dochter. Maar er is gewoon ergens een simkaartje gekocht met een mobiele telefoon. En je telefoonnummer is bijvoorbeeld bekend door een datalek bij -weet ik het- een hotelbedrijf of een schouwburg, dan kun je een appje krijgen met zo'n Tikkie of betaalverzoek. Dus ja, het Tikkie en betaalverzoek is veilig. Je moet je alleen goed afvragen: van wie krijg ik het en wil ik deze betaling wel doen?
00:17:37
Zegert van der Linde: Ja, heb ik inderdaad dat cadeautje gekocht voor iemand en moet ik daar nog €15 voor betalen? Of meer, want ik weet niet of oplichters voor maar €15 gaan.
00:17:47
Peter Rollé: En daarbij wordt met name Tikkie misbruikt voor phishing. Dus dat betekent eigenlijk dat, ik noemde net al bijvoorbeeld Marktplaats, je contact hebt met iemand en die zegt: "Hierbij heb je een betaalverzoek om bijvoorbeeld die betaling te doen." Ja, dan kan zo'n Tikkie -het ziet er dan uit als een Tikkie link- misbruikt worden voor bijvoorbeeld phishing. Dus dan denk jij: ik krijg een app met bijvoorbeeld een betaalverzoek, een Tikkie of een PostNL label. Als je daar uiteindelijk op klikt -en dan moet je weer op die URL letten- word je doorgeleid naar een valse website.
00:18:23
Zegert van der Linde: Ja, goed opletten dus weer.
00:18:24
Peter Rollé: Ja, wij noemen dat dan een nep-Tikkie.
00:18:25
Zegert van der Linde: Dat is het eigenlijk ook, ja. En dan kan het toch een keer misgaan, weet je wel. Daar kun je dan wel heel stom over voelen, maar ik vraag me dan wel af -en ik denk misschien ook wel dat het waar is-: kan het iedereen overkomen?
00:18:42
Peter Rollé: Het gebeurt helaas steeds meer. Je ziet met name in 2020 op gebied van online fraude, dus cybercriminaliteit, valse linkjes, bankhelpdeskfraude, dus dat mensen gebeld worden door de bank van: "Uw geld is niet veilig, u moet het zelf even overboeken naar zogenoemde kluis." Maar ook de WhatsApp oplichting. Je ziet heel veel diversiteit aan manieren van oplichting. Jij noemde het in het begin al: de zwakste factor is dan toch helaas de mens, die handelt uit emotie. Er is paniek gecreëerd door de oplichters, bijvoorbeeld: mijn geld is niet veilig of mijn zoon is in nood. Dat zet mensen toch aan om die betalingen te doen. Dus als je het hebt over het feit dat mensen slachtoffer worden, ja, de laatste jaren helaas steeds meer. En als wij slachtoffers spreken bij de bank, dan is er heel veel schuldgevoel, want soms is ook in hun omgeving veel onbegrip voor het feit dat mensen zich hebben laten oplichten. Maar besef je goed: dat is soms met de goede intenties gedaan, soms door hele slinkse werkwijze van de

oplichters. Er wordt vertrouwen gecreëerd. Ik heb bijvoorbeeld ook een keer een opname gehoord van iemand die is opgelicht per telefoon. Het is gewoon zo goed gedaan. De oplichter had bij wijze van spreken zo bij de bank in de klantenservice kunnen werken, want die was zo vriendelijk.

00:20:05

Zegert van der Linde: Was hij dat maar gaan doen.

00:20:07

Peter Rollé: Ja, was hij dat maar gaan doen. Dan dat hij mensen kunnen helpen in plaats van kunnen bestelen. Dus ja, er is ook een instantie, Slachtofferhulp Nederland, die slachtoffers opvangt. En je ziet met name in de coronatijd, ze hebben het heel druk met slachtoffers door cybercriminaliteit. En je ziet bijvoorbeeld veel minder inbraken en dat soort zaken. Dus diefstal…

00:20:30

Zegert van der Linde: Op een andere manier.

00:20:31

Peter Rollé: Verplaatst zich van... Ja, op een andere manier. Maar ja, de criminelen hebben het nog altijd druk, denk ik.

00:20:36

Zegert van der Linde: Maar slachtofferhulp zelfs?

00:20:37

Peter Rollé: Zeker.

00:20:37

Zegert van der Linde: Zo heftig kan het dus zijn voor mensen?

00:20:39

Peter Rollé: Ja, soms moet er echt psychologische hulp komen om dingen te verwerken.

00:20:45

Zegert van der Linde: Zo, jeetje. Dat is heftig, maar er is natuurlijk ook een praktische kant aan als dit gebeurt. Het is je overkomen, je hebt geld overgemaakt naar de verkeerde persoon, op wat voor manier dan ook. Wat moet je doen?

00:20:54

Peter Rollé: Het eerste wat ik zou adviseren, is contact op te nemen met de bank. Wij noemden dat al eerder natuurlijk: geld is heel snel momenteel. Binnen twee, drie seconden heb je een overboeking gedaan, of dat nou via Tikkie gaat of gewoon een normale overboeking. Het is heel belangrijk direct contact te zoeken met de bank. Soms is er mogelijkheid om bijvoorbeeld het geld te blokkeren bij degene die het heeft ontvangen. Maar ja, je moet wel besef hebben dat, op het moment dat je wordt opgelicht, degene die jou aan het oplichten is als het ware klaarstaat met de pinpas van de rekening waar het op gestort moet worden om het op te nemen. Soms zie je er een aantal minuten tussen zitten en geld is vaak weg. Maar bel altijd de bank, want dan kunnen wij ook die andere rekening blokkeren. Dus op het moment dat jij bijvoorbeeld slachtoffer wordt van neem WhatsApp oplichting en jij neemt geen contact op met de bank, dan kan die boef die rekening langer gebruiken voor oplichting tot hij geblokkeerd wordt. En als jij direct belt en soms is het geld al weg, dus daar doe je het dan helaas niet meer voor, maar je helpt wel anderen beschermen. En daarna uiteraard aangifte doen bij de politie.

00:22:04

Zegert van der Linde: Altijd aangifte doen. Je bent opgelicht, er is geld van je gestolen. Dus altijd contact opnemen met je bank. Dan als afsluiting, wat zijn nou voor jou, wat jou betreft de beste tips als je online je financiële zaken regelt?

00:22:18

Peter Rollé: Besef je goed, voordat je die betaling doet... We noemden in het begin de acceptgiro of het overschrijvingskaartje, daar zette je je handtekening op. Tegenwoordig met de Touch ID en vijfcijferige codes wordt die handtekening heel snel gezet. Als je gaat signeren, om het even zo te noemen, kijk dan gewoon even goed: wat betaal ik nu eigenlijk, aan wie en waarom? En klopt het wel dat dit normaal is wat ik doe? Daarbij is het zo dat de banken nooit zullen vragen om geld over te boeken. Dat doen wij of wij blokkeren de rekening als er sprake is van fraude of onveiligheid. En vertrouw ook niet mensen die bijvoorbeeld aan de deur komen om een pas te wisselen.

Kijk, banken hebben gewoon een veilige manier van bankieren gecreëerd. Maar laat je niet verleiden door handelingen die je nog nooit hebt gedaan. En bij twijfel, nogmaals, bel je bank.

00:23:12

Zegert van der Linde: Bel je bank.

00:23:13

Peter Rollé: En klik niet klakkeloos.

00:23:14

Zegert van der Linde: Klik niet klakkeloos.

00:23:17

Peter Rollé: Dat vond ik een hele mooie. Die hoorde ik laatst.

00:23:17

Zegert van der Linde: Ja, dat is een hele goeie. Die zit ook in aflevering één met Esther Mieremet inderdaad. Klik niet klakkeloos. Heel goed. Peter Rollé, dank je wel.

00:23:21

Peter Rollé: Graag gedaan.

00:23:26

Zegert van der Linde: Dit was de derde aflevering van de SeniorWeb Podcast. U luisterde naar een gesprek met Peter Rollé van de Rabobank over online bankieren en betalen. Wilt u meer tips en informatie over online veiligheid? Kijk dan op www.seniorweb.nl en klik op Online veiligheid en privacy. Wilt u de SeniorWeb Podcast volgen, dan kan dat het makkelijkste via een podcast app op uw telefoon. Kijk voor een uitleg op seniorweb.nl/podcast. Volgende week is er een nieuwe aflevering. Voor nu, bedankt voor het luisteren en tot de volgende keer.