Dwars door het recht met HJS

Het Juridisch Spreekuur (HJS) van de Hogeschool van Amsterdam (HvA) behandelt in deze rubriek actualiteiten die met het recht te maken hebben.

Phishing?

Tekst: HJS-medewerker Zanilya Hollingsworth

Phishing is een vorm van digitale oplichting, fraudeurs doen dit door gebruik te maken van sms-berichten of het verzenden van berichten via de e-mail of Whatsapp. Slachtoffers worden bijvoorbeeld naar een onveilige website gelokt, waar vervolgens bank- of andere inloggegevens worden gevraagd en prijsgegeven. Of men maakt geld over naar het rekeningnummer van een fraudeur die zich voordoet als een (overheids-) instantie en/of andere organisatie.

Het komt zelfs voor dat men denkt met een familielid in zee te gaan. In het bericht kan staan dat u bijvoorbeeld een rekening moet betalen, dat er iets mis is met uw bankgegevens of dat uw bankpas is verouderd en dat u gratis een nieuwe kunt aanvragen.
Criminelen lokken u vervolgens naar een valse website, die op het eerste oog niet vals blijkt te zijn. Na het prijsgeven van uw persoonlijke/vertrouwelijke gegevens krijgt de fraudeur de beschikking over deze gegevens. Het kwaad is dan geschied, u kan dan bijvoorbeeld het overgemaakte geldbedrag niet meer terugboeken of uw bankrekening wordt leeggehaald.

Voorkom dat u slachtoffer wordt van phishing

Reageer nooit op mails of berichten waarin u wordt verzocht om persoonlijke gegevens, inlogcodes of een pin-code te verstrekken. De diverse (overheids-)organisaties en instanties zullen u nooit via een e-mail, sms- of WhatsApp-bericht verzoeken om deze informatie en/of vragen een openstaande rekening te voldoen.

Enkele tips:

- Ontvangt u een phishing-mail of bericht? Verwijder deze dan meteen.
- Klik nooit op een link die in de e-mail of het bericht staat.
- Ontvangt u oproepen en/of betaalverzoeken van onbekenden, negeer deze en blokkeer deze beller.
- Ga nooit in op het verzoek om uw (oude) bankpas die verloopt toe te zenden. Als u een nieuwe pas toegezonden krijgt, dan zal de bank u altijd vragen om uw oude pas door te knippen en zelf weg te gooien.
- Verstuur ook nooit een kopie van uw identiteitsbewijs naar derden. Criminelen kunnen uw BSN-nummer gebruiken om een bankpas aan te vragen.
- Rijbewijs behaald? Zet hiervan geen foto op een van de sociale mediakanalen (zoals bijvoorbeeld Facebook, Instagram of Twitter). De zichtbare persoonsgegevens op de foto van het rijbewijs kunnen daarna door fraudeurs worden misbruikt.
- Geef nooit zomaar persoonlijke gegevens door als iemand u telefonisch – of aan de deur benadert.
- Vertrouwt u een link niet helemaal, check deze via de website www.checklinkje.nl of download de app: Opgelicht.
- Herken valse e-mails. Dit kunt u controleren door middel van te kijken naar link(s), verdachte afzenders, onderwerpen en/of kwaadaardige bijlagen. Voor meer info zie de site van de Consumentenbond: www.consumentenbond.nl/veilig-internetten/nepmails-en-phishing.
- Zorg dat uw wachtwoorden veilig zijn en verander ze regelmatig.
- Wees er zeker van dat uw computer de laatste software- en beveiligingsupdates heeft gehad.

Het team van HJS

Wat kunt u doen als u slachtoffer bent geworden van phishing?

Heeft u een bijlage geopend en u vertrouwt het achteraf niet? Laat uw computer, tablet of smartphone controleren op schadelijke software. Daarna kunt u het beste uw wachtwoorden wijzigen.

- Wacht met internetbankieren tot u zeker weet dat uw computer weer “schoon” is.
- Nadat u heeft gemerkt slachtoffer te zijn geworden van phishing, is het verstandig om direct uw bank te bellen, zodat er actie kan worden ondernomen.
- Doe aangifte van phishing bij de politie.
- Er bestaat een fraudehelpdesk (www.fraudehelpdesk.nl). Het is ook verstandig om de desbetreffende organisatie of instantie van uw fraudebevindingen op de hoogte te stellen. Bovendien kunnen deze organisaties of instanties zodoende zicht houden op de laatste ontwikkelingen en een breder publiek waarschuwen via de eigen website. Hoe meer meldingen, hoe groter de kans dat de politie er ook mee aan de slag gaat.

Waar(mee) kan HJS u (verder) nog helpen?

Medewerkers van HJS staan voor u klaar om al uw vragen over phishing, andere juridische en sociaal-maatschappelijke kwesties te beantwoorden. Als blijkt dat het niet mogelijk is om uw vraag te beantwoorden, dan verwijzen wij u door naar een van onze samenwerkingspartners.
U kunt hiervoor terecht op de onderstaande locaties, maar neem gelet op het feit dat we in “een coronatijdperk leven” eerst telefonisch contact op met een van de HJS-medewerkers op onderstaande nummers. Bij de locaties nemen wij de geldende RIVM-voorschriften in acht. #

BOOT-Oost: HJS-spreekuurtijden: Sumatrastraat 314 (1095 HV) telefoon: 020 - 233 97 59
Inloopspreekuur: elke dinsdag van 13:00 tot 17:00 uur

HJS: Wibautstraat 5a (Muller Lulofshuis)2e etage (02A08)telefoon: 06 - 211 588 82
Bereikbaar & inloopspreekuur: maandag t/m donderdag van 9:00-17:00 uur
e-mail: hjs@hva.nl, twitter: @hva-hjs, website: www.hva.nl/hjs