



Cyber Safety

life  beats

lyondellbasell

Hoe kwetsbaar is jouw Online Identity?

- Delen van de aanbevolen software en oplossingen, in deze presentatie, zijn ter informatie en kunnen alleen worden geïnstalleerd op **je persoonlijke** computer (niet op een LyondellBasell computer) **voor eigen risico**. LyondellBasell of een van haar entiteiten kunnen niet verantwoordelijk worden gehouden voor interne of externe schade aan je apparatuur of data.



Je on-line identiteit is je paspoort om gebruik te maken van miljoenen services die on-line beschikbaar zijn. Variërend van email tot zakelijke applicaties, webwinkels en mobiele telefoons.

Heb je ooit nagedacht over de risico's waaraan je on-line identiteit is bloot gesteld?



De risico's van E-mail



- Eén Email Account voor alles wat je doet.
 - Lastig om te navigeren tussen de legitieme mails en “andere mails” die je ontvangt
 - Kwetsbaar – indien je dit account verliest is er meestal geen “plan B”
 - Gebrekkige bescherming tegen moderne phishing emails

Je hoeft je email alleen maar bekend te maken!

Wat is Phishing?

Phishing is een van de meest voorkomende aanvallen, via je email account, waarbij cyber aanvallers proberen om je een actie te laten uitvoeren waardoor je gegevens onthult.



Hoe kun je voorkomen dat jouw email account risico loopt?

- Gouden Regel – Naar mate je emailadres meer bekendheid krijgt, ontvang je ook meer SPAM en phishing emails.
- Daarom is het raadzaam om meerdere emailadressen te hebben voor verschillende doeleinden.
 - Persoonlijke communicatie
 - Groepsemail
 - Reclame
 - Eenmalige aankopen
 - Online winkelen
- Schrijf alleen in op wat echt belangrijk is. Vermijd last minute “drop your business card” aanbiedingen.
- Indien je ergens voor inschrijft via je emailadres, HERGEBRUIK NOOIT PASSWORDS.

Passwords – Risico's uit de praktijk



- Passwords († RIP)
 - Hergebruik nooit je password
 - Criminelen laten programma's lopen om user names and passwords te achterhalen via diverse websites
 - Zelfs als je het risico wil nemen; wat gebeurt er als je provider wordt gehackt?
 - Als je ooit heb ingelogd op een publieke computer (internet café, hotel) loop je meer risico dat jouw gegevens in handen van criminelen belanden.

Bescherming van je Passwords

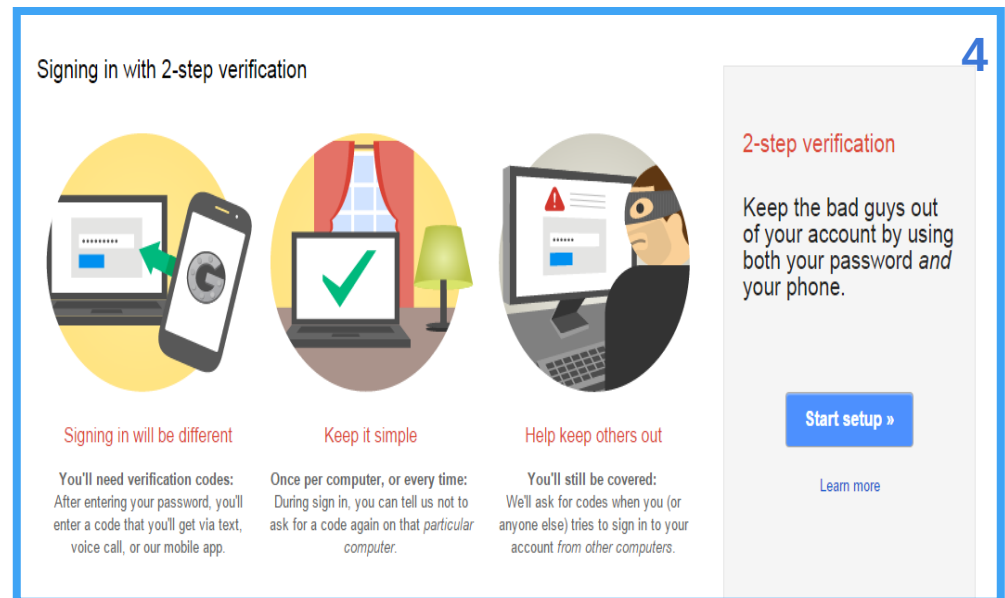
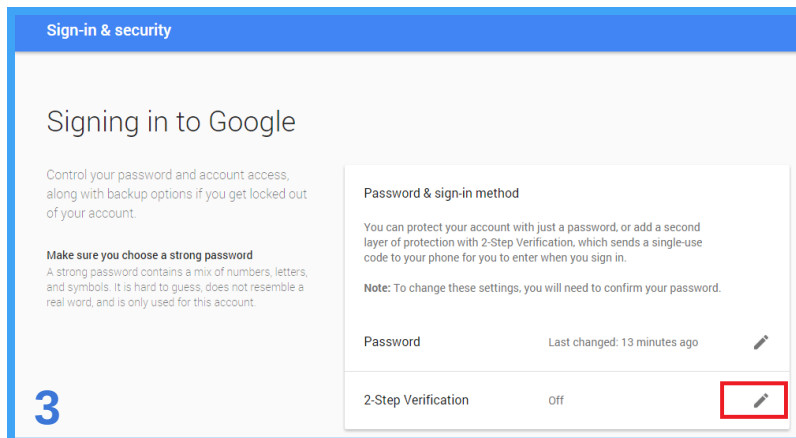
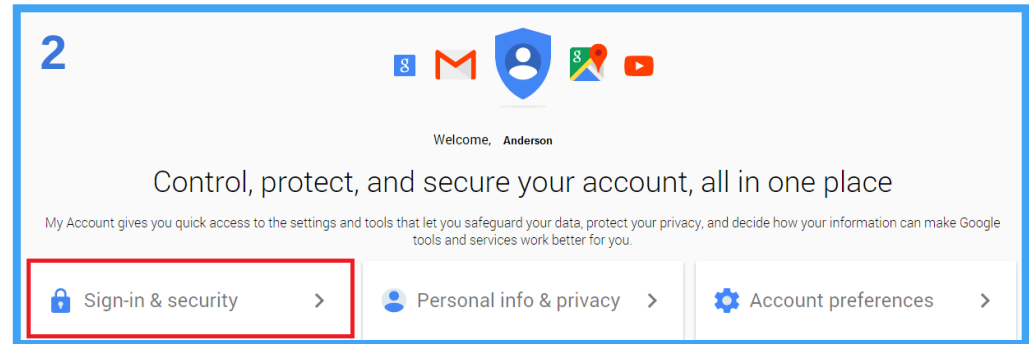
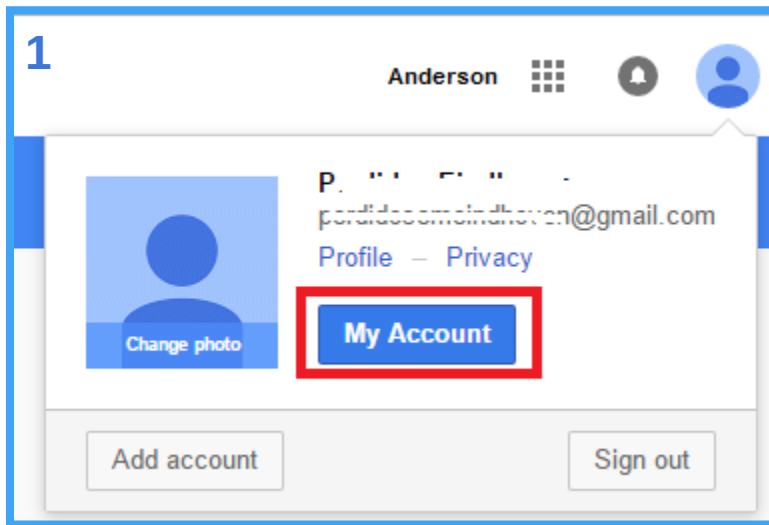
- **Nooit**, je passwords hergebruiken
- Bouw bij inschrijving voor bepaalde diensten altijd een **tweede herkennings factor** in (eenmalig password, SMS'je of zelfs bevestigsemail naar een tweede emailaccount.
- Het inschakelen van password bewaarders kan nuttig zijn wanneer ze gebruik maken van geavanceerde technieken en je password niet via het web heen en weer sturen.
- Laat je apparatuur nooit ongeheerd achter zonder password bescherming.

Afscherming van je email – Door toevoeging van 2 ledige herkenning factor

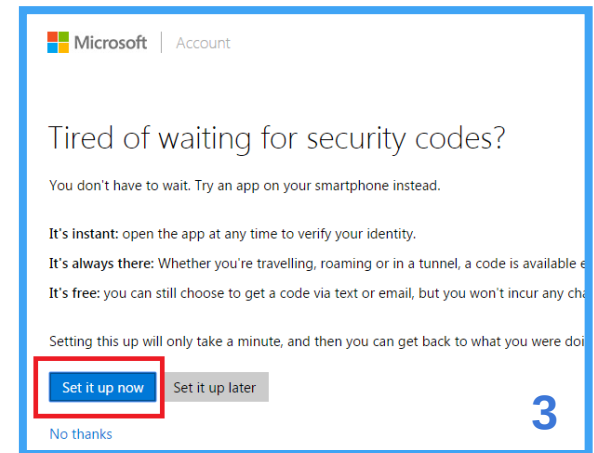
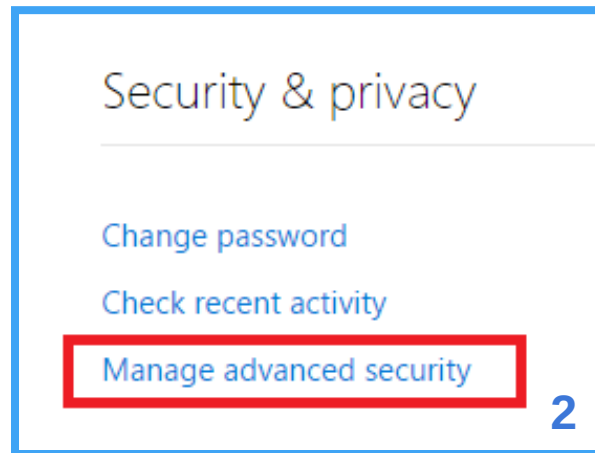
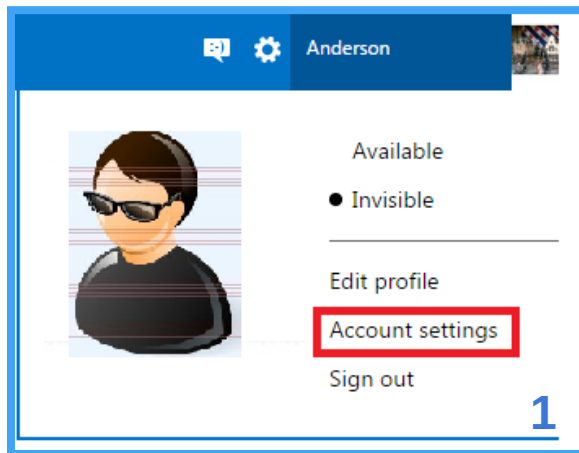
- Om in te loggen bij je email provider wordt je meestal gevraagd om een enkele herkenning factor. Meestal een password.
- Als een hacker achter je password komt is het vrij zeker dat hij in staat is om zich toegang te verschaffen tot je emailaccount, behalve...



Inschakelen van Google 2 Factor Authentication Stap-voor-Stap



Inschakelen van Google 2 Factor Authentication Stap-voor-Stap



Set up an authenticator app for your iPhone, iPad or iPod touch

1. Install Google's authenticator app, or search for "authenticator" in your app store. (This link will open in a new tab.)
2. Open the app.
3. Pair the app with your Microsoft account by scanning this barcode.



[I can't scan the barcode](#)

4. Verify that the pairing was successful by entering a code below.

Code generated by app

Next

Skip

Don't have an iOS device? Go back to pick a different device.

4

Setting up an authenticator app for your Windows Phone

1. Install Microsoft's authenticator app. (This link will open in a new tab.)
2. Open the app.
3. Pair the app with your Microsoft account by scanning this barcode.



[I can't scan the barcode](#)

4. Verify that the pairing was successful by entering a code below.

Code generated by app

Next

Skip

Don't have a Windows Phone? Go back to pick a different device.

4



- Alleen staande computer met meerdere gebruikers.
 - Verschillen in gebruik vereisen ook verschillende veiligheids niveau's;
 - Het is bewezen dat sites voor spelletjes en porno vaak gebruikt worden door criminelen om virussen en malware te plaatsen.
 - Vertrouw je de computer van een vriend? Beveiligt hij zijn computer net zo goed als jij?
- Wees voorzichtig met het aansluiten van externe apparaten of met DVD's van buitenstaanders. Virusinfectie ontstaat vaak door USB sticks.

A black Samsung smartphone is shown at an angle, displaying the Candy Crush game. The screen features the game's title, a colorful landscape with a pink unicorn, and a 'Play' button. The phone is resting on a light-colored wooden surface.



≠



Hoe voorkom ik dat mijn computer risico loopt?

- Scheidt zakelijk van plezier; Je kunt niet, zonder risico, beiden doen op een computer. Dit geldt ook voor je mobiele apparatuur.
- Deel geen computer! Een fout van de ene kan een probleem worden voor de ander – Dit omvat alle gedeelde computer in b.v. hotels en internet café's.
- Schaf een compleet beveiligingssysteem aan (Firewall, Antivirus, AntiSpam) een stel OS (Windows, Android, Mac OSX, or Linux XYZ)in staat om automatische updates uit te voeren.
- Voorkom downloading of het binnen halen van software van onbekende bronnen of gedeeld via vrienden.
- Houdt je computer Software Up-to-Date door de vereiste antivirus updates te installeren.

Cyber Safety

Je hebt het zelf in de hand!

Start Vandaag.



Authored by: Anderson Domingues (LBR) & Suzanne Jurczik (LBR)