Cyber Safety

life beats

lyondellbasell

How Fragile is Your Online Identity?

Some of the software and solutions indicated on this presentation are solely for ***informational purposes*** *and can only be installed at* ***your personal computer*** *(not on any LyondellBasell devices)* ***at your own risk.*** *LyondellBasell or any of its entities cannot be held liable in case of any logical or physical damages caused to your equipment or data.*

Your on-line identity is your passport to interact with millions of services available on-line, ranging from e-mail to enterprise applications, web stores and even cellphones.

Have you ever thought about the risks of losing or exposing your online identity?

E-mail Risks

- A Single Email Account for Everything You Do
  - Hard to navigate between the legitimate and “other stuff” you receive
  - Single point of failure – If you lose that email account there is usually no “plan B”
  - Deficient mechanisms for preventing modern email phishing

All you need to do is give your email away!

What is Phishing?

Phishing is one of the most common email based social engineering attacks. It is a technique where cyber attackers attempt to fool you into taking an action or divulging information.

How to Not Put Your Email at Risk?

- Golden Rule – The more public your email becomes, the more SPAM and phishing emails you will receive.

- Have different email accounts for different purposes.
  - Personal communication
  - Communication lists
  - Promotions
  - One time buys
  - Online shopping

- Only signup for what is really relevant. Avoid last minute “drop your business card” offers.

- Whenever signing up for a service with your email, NEVER REUSE PASSWORDS.

Passwords – Practical Risks

- Passwords († RIP)
  - Never reuse it!
  - Criminals run scripts able to check usernames and passwords across multiple websites.
  - Even if you accept the risks, what if one of your providers get hacked?
  - Have you ever used it on a cyber café, hotel or at any other shared computer? There are very high chances your credentials are already in criminal hands.

Protecting Your Passwords

- **Never**, under any circumstance, reuse your passwords.

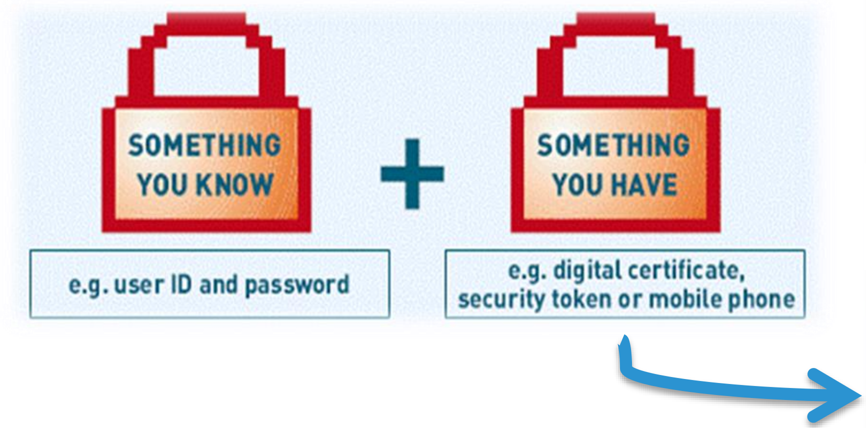
- When subscribing for online services always look for a **second authentication factor** (one-time password, calls, SMS's or even emails to a secondary account.

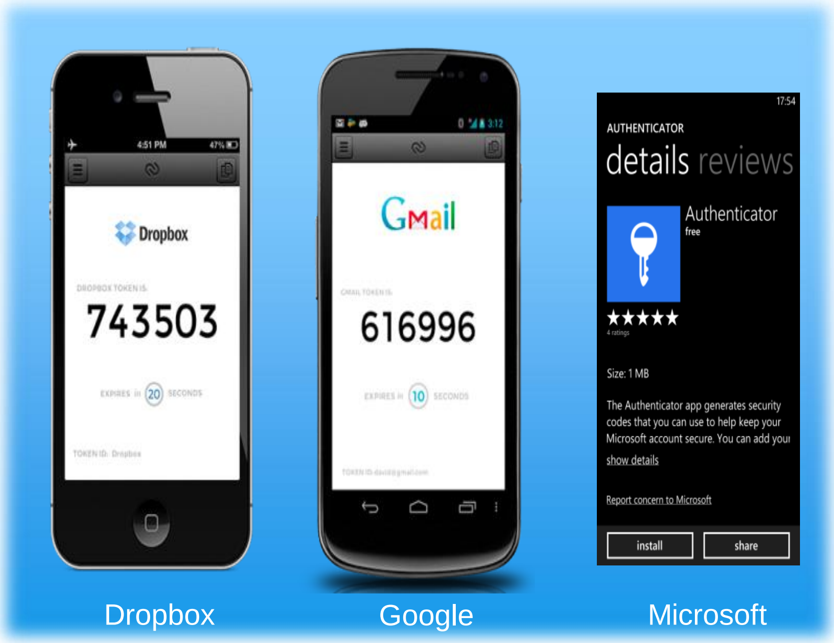
- Use of Password Keepers can be useful when they make use of advanced encryption and do not transport your password back and forth on the internet.

- Avoid leaving your smart devices without any password protection.

Shielding Your E-mail – Adding Two Factor Authentication

- To Login on your e-mail provider you're usually required to provide a **single authentication factor**, usually this is **something** that **you know** like a password for example.
- Obviously if a hacker obtains access to your password it is almost sure he will be able to access your e-mail, unless…

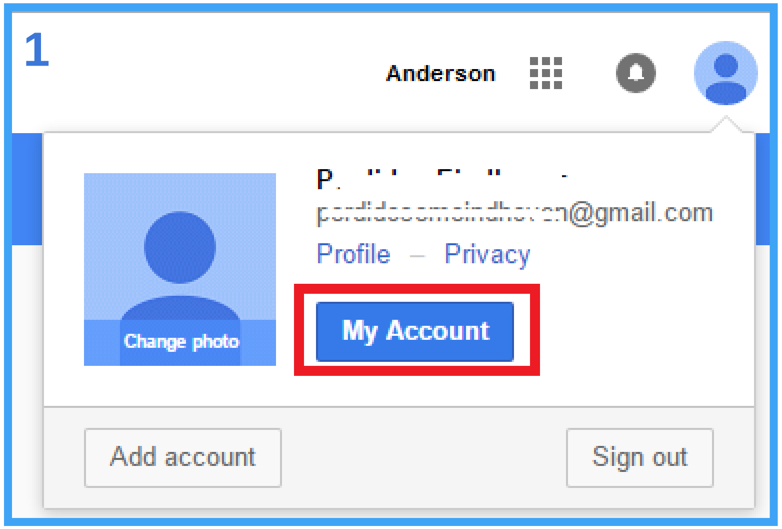

SOMETHING YOU KNOW
+
SOMETHING YOU HAVE
e.g. user ID and password
e.g. digital certificate, security token or mobile phone



The Authenticator app generates security codes that you can use to help keep your Microsoft account secure. You can add your

Dropbox Google Microsoft

Enabling Google 2 Factor Authentication Step-by-Step

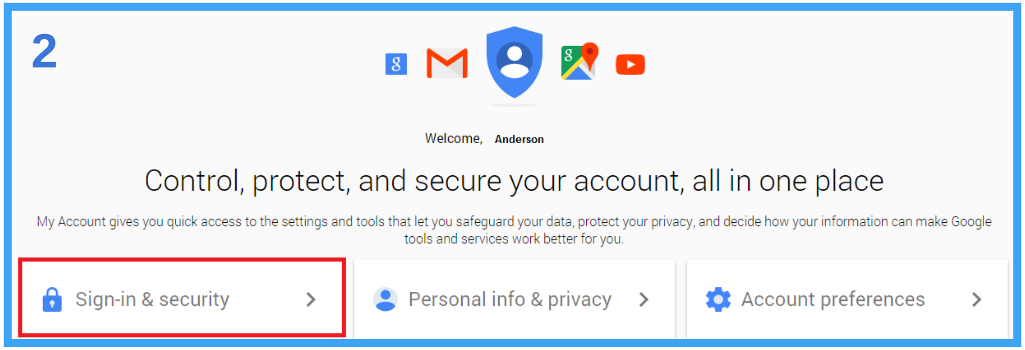


1

Anderson

[redacted]

[redacted]n@gmail.com

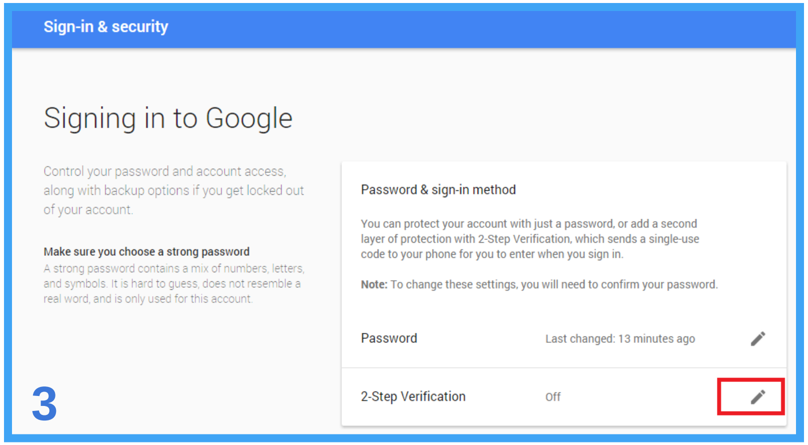


2

Welcome, Anderson

Control, protect, and secure your account, all in one place

My Account gives you quick access to the settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google tools and services work better for you.



3

Signing in to Google

Control your password and account access, along with backup options if you get locked out of your account.

Make sure you choose a strong password

A strong password contains a mix of numbers, letters, and symbols. It is hard to guess, does not resemble a real word, and is only used for this account.

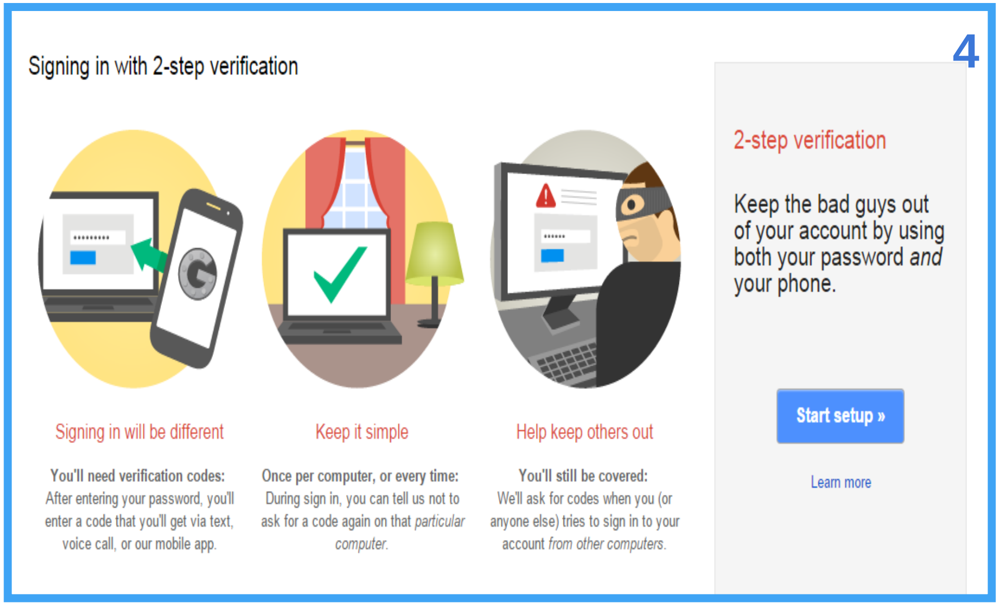
Password & sign-in method

You can protect your account with just a password, or add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in.

Note: To change these settings, you will need to confirm your password.

Password Last changed: 13 minutes ago

2-Step Verification Off



4

Signing in with 2-step verification

Signing in will be different

You'll need verification codes: After entering your password, you'll enter a code that you'll get via text, voice call, or our mobile app.

Keep it simple

Once per computer, or every time: During sign in, you can tell us not to ask for a code again on that *particular computer.*

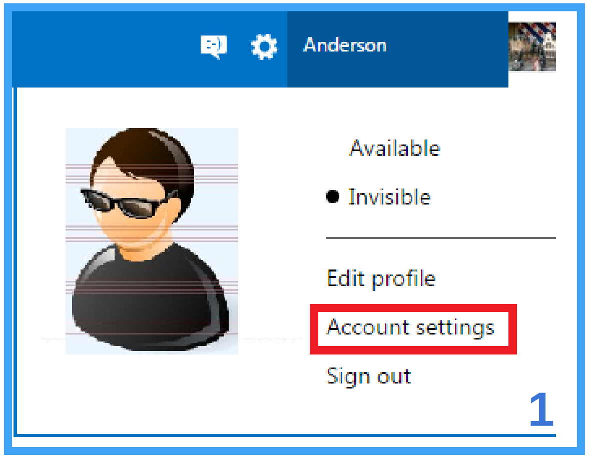
Help keep others out

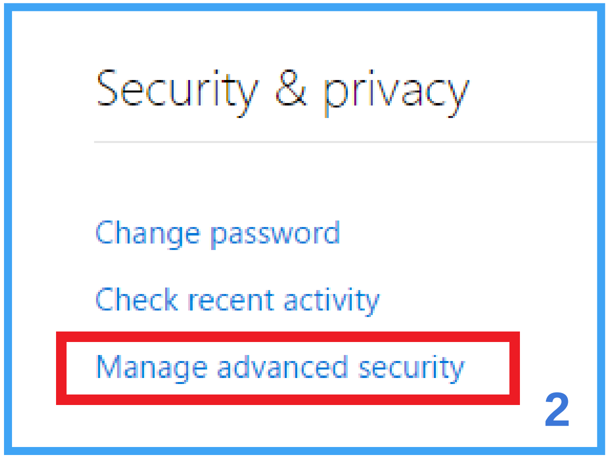
You'll still be covered: We'll ask for codes when you (or anyone else) tries to sign in to your account *from other computers.*

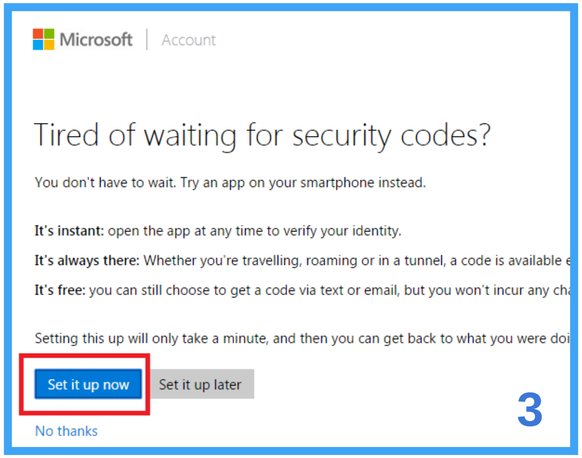
2-step verification

Keep the bad guys out of your account by using both your password *and* your phone.

Enabling Microsoft 2 Factor Authentication Step-by-Step




Security & privacy



Tired of waiting for security codes?

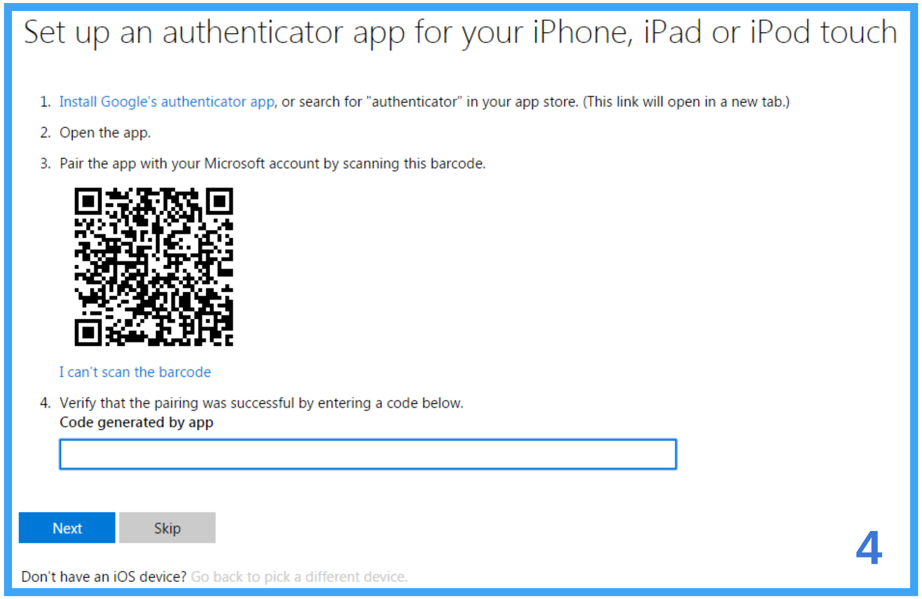
You don't have to wait. Try an app on your smartphone instead.

It's instant: open the app at any time to verify your identity.

It's always there: Whether you're travelling, roaming or in a tunnel, a code is available e

It's free: you can still choose to get a code via text or email, but you won't incur any ch

Setting this up will only take a minute, and then you can get back to what you were doi


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

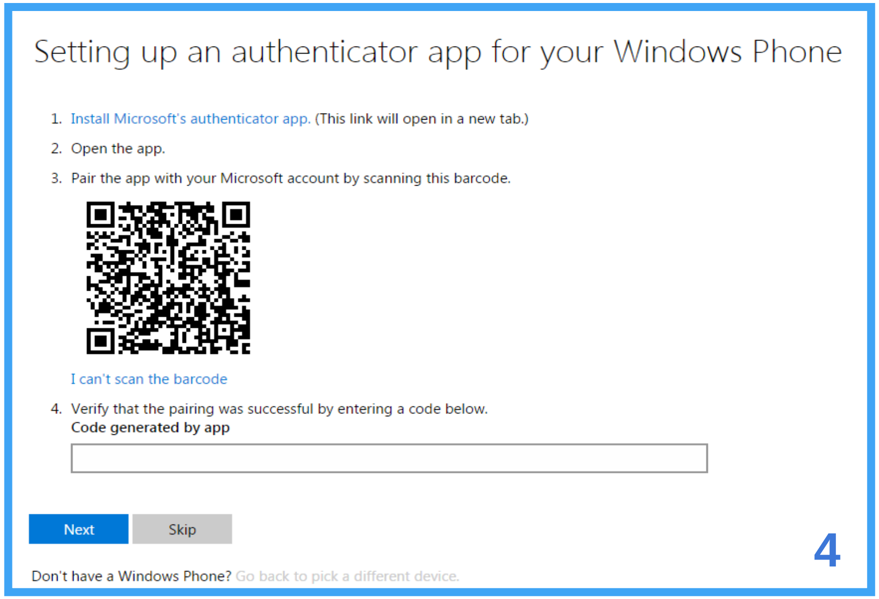
1. Install Google's authenticator app, or search for "authenticator" in your app store. (This link will open in a new tab.)
2. Open the app.
3. Pair the app with your Microsoft account by scanning this barcode.

I can't scan the barcode

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

Code generated by app

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


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

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

Home Computers – Practical Risks

- Single computer with multiple users
  - Different types of access require different security levels;
  - It is proven (piracy, gaming and porn) are frequently used by criminals to plant virus and malware.
  - Do you trust your friend’s computer? Does he care about his computer the same way you do?

- Be careful about connecting storage devices or DVD’s from other parties. Virus infection through USB sticks is still a very common technique.

Multi-Purpose But… With Limitations

≠

How to Not Put Your Computer at Risk?

- Separate Business from Fun; you cannot do both on the same device without embracing serious risks. The same is applicable to your mobile devices.
- Don’t Share Computers! One’s mistake can be another’s problem – This includes conference computers and computers from Hotels and Cyber Cafés.
- Buy a Complete Security Solution (Firewall, Antivirus, AntiSpam) and enable OS (Windows, Android, Mac OSX, or Linux XYZ) automatic updates.
- Avoid downloading or obtaining software from Unknown Sources or shared by friends.
- Always Keep your Computer Software Up-to-Date by installing the required patches and antivirus updates.

Cyber Safety

Cyber Safety

It’s in Your Hands!

Start Today.

life beats

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