



Seguridad Cibernética

life  beats

lyondellbasell

¿Qué tan frágil es su identidad en línea?

Algunos de los programas y soluciones indicados en esta presentación son completamente con **propósito informativo** y solo puede ser instalado en su **computadora personal** (no en equipo de LyondellBasell) **bajo su propio riesgo**. LyondellBasell o cualquiera de sus entidades no pueden ser responsables en caso de daños físicos o lógicos causados en su equipo o en su información.



Su identificación en línea es su pasaporte para interactuar con millones de servicios disponibles en línea, que van desde correo electrónico a aplicaciones empresariales, tiendas web e incluso celulares.

¿Ha pensado acerca del riesgo de perder o exponer esa identidad?



Riesgo de Correo Electrónico



- Una sola cuenta para todo lo que hace
 - Difícil de navegar entre correos legítimos y “todo lo demás” que reciba
 - Punto único de fallo – si llega a perder esa cuenta por lo general no existe un “plan B”
 - Mecanismos deficientes para la prevención moderna de phishing de correo electrónico

Todo lo que necesita hacer es dar su correo!

¿Qué es Phishing?

El phishing es uno de los ataques más comunes de ingeniería social basada en correo electrónico. Es una técnica donde los atacantes cibernéticos intentan engañar, haciendo que tome una acción o por la divulgación de información.



¿Cómo no poner su correo en riesgo?

- Regla de Oro – Entre mas publico se hace su correo, recibirá mas correos de SPAM y de Phishing.
- Tenga varias cuentas para diferentes usos.
 - Comunicaciones personales
 - Lista de comunicaciones
 - Promociones
 - Compras de una sola vez
 - Compras en línea
- Solo regístrese para o que valga la pena. Evite las ofertas de “Deje su tarjeta de negocios” de ultimo minuto.
- Cuando se registre por un servicio con su correo, **NUNCA REPITA CONTRASEÑAS.**

Riesgos Prácticos - Contraseñas



- Contraseñas († RIP)

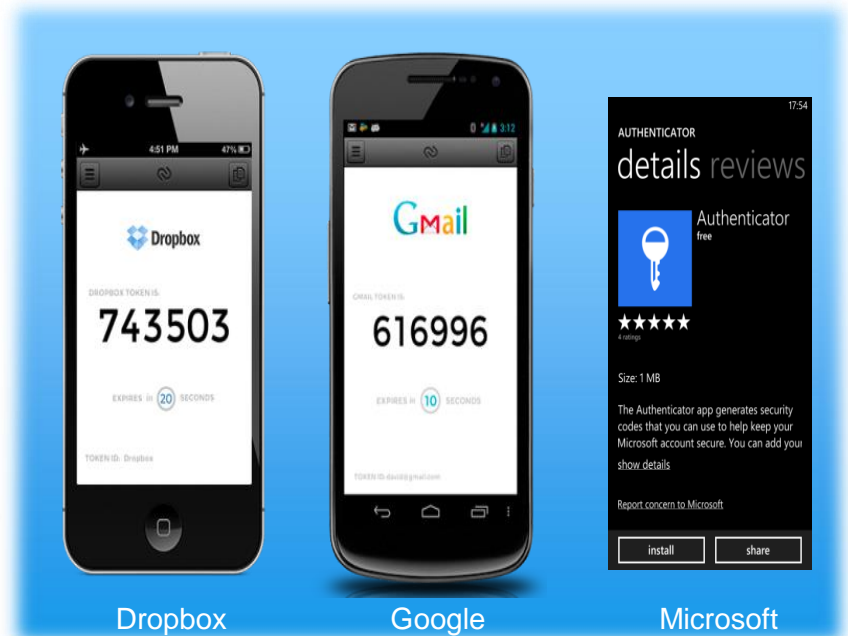
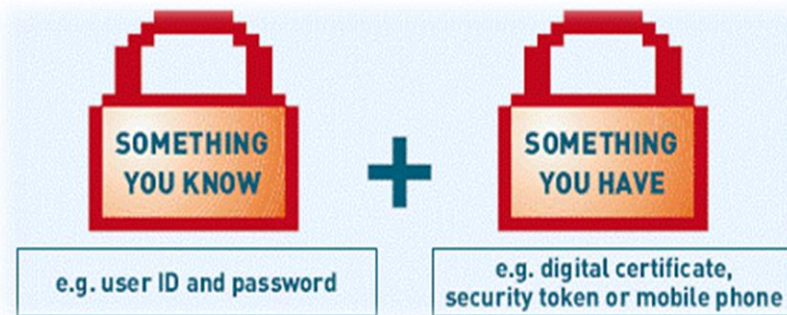
- Nunca lo vuelva a usar!
- Los delincuentes ejecutan secuencias de comandos capaces de comprobar nombres de usuario y contraseñas a través de múltiples sitios web.
- Incluso si acepta los riesgos, ¿que pasara si uno de sus proveedores es hackeado?
- ¿Alguna vez la ha utilizado en un café cibernético, hotel o en cualquier otro equipo compartido? Hay posibilidades muy altas de que sus credenciales ya estén en manos criminales

Proteja sus contraseñas

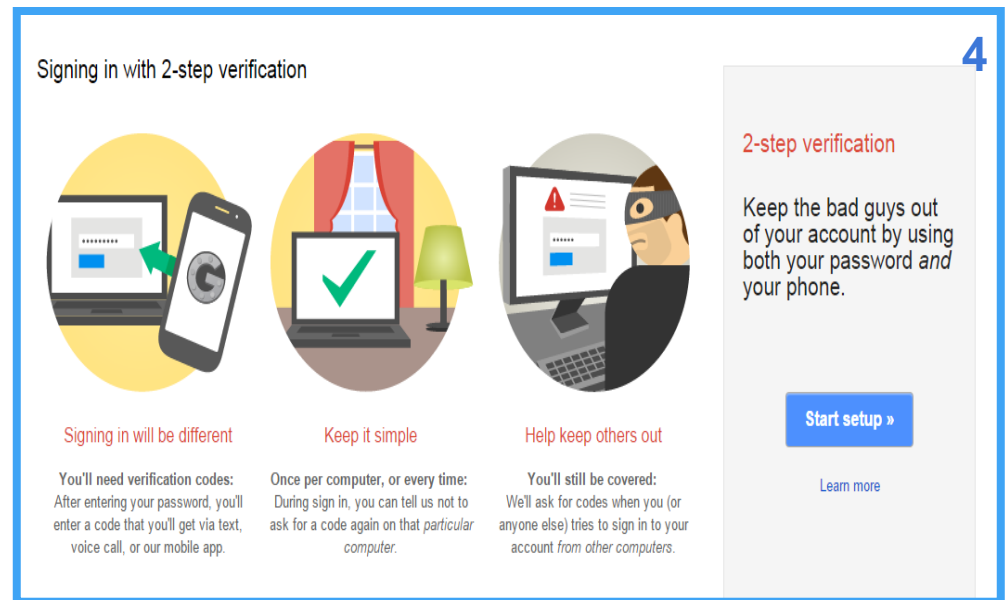
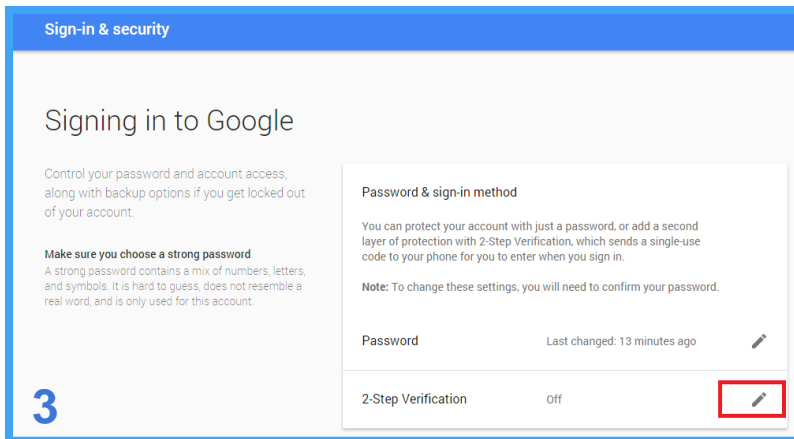
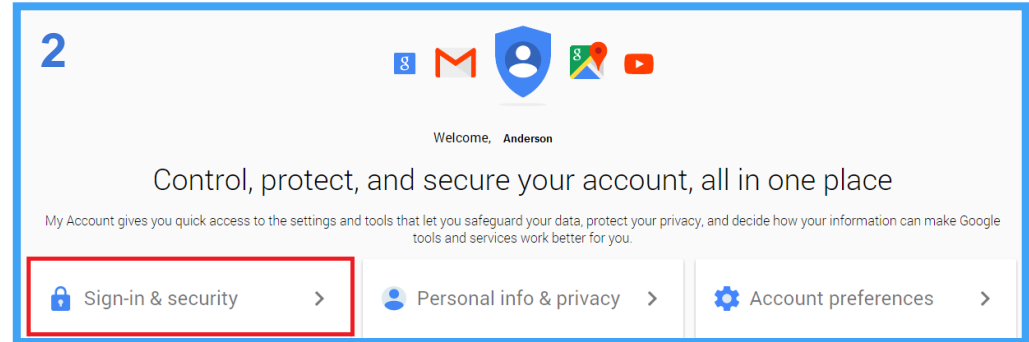
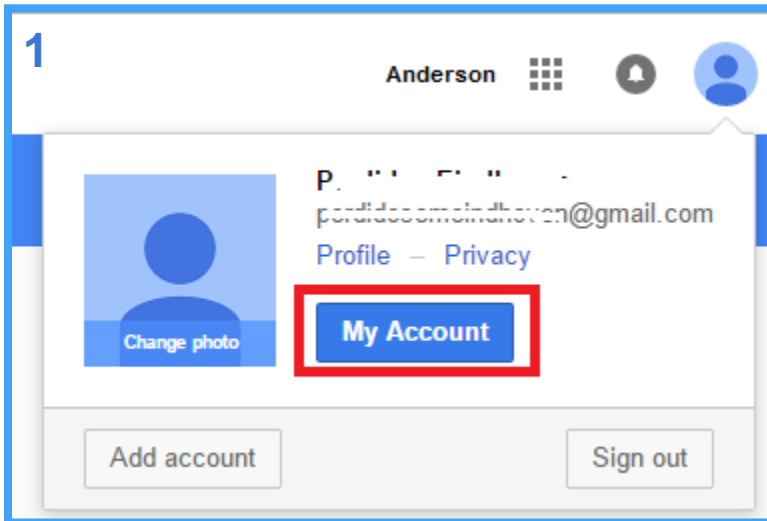
- **Nunca**, bajo ninguna circunstancia, vuelva a utilizar contraseñas.
- Cuando se suscriba a servicios en línea siempre busque un segundo factor de autenticación (contraseña de un uso, llamadas, SMS o incluso mensajes de correo electrónico a una cuenta secundaria)
- Use Guarda Contraseñas puede ser útil cuando haga uso de encriptación avanzada y así no transporte su contraseña de un lado a otro en el Internet.
- Evite dejar sus dispositivos inteligentes sin ningún tipo de protección de contraseña.

Proteja su Correo – Agregue un factor doble de autenticación

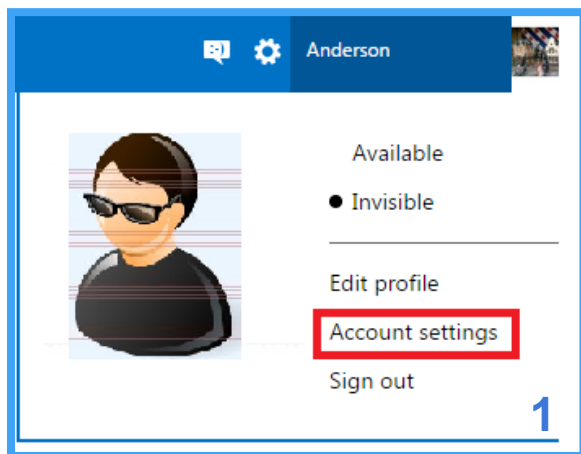
- Para entrar su correo su proveedor por lo general requiere que proporcione un único factor de autenticación, por lo general esto es una contraseña, por ejemplo.
- Obviamente, si un hacker obtiene acceso a su contraseña es casi seguro de que será capaz de acceder a su correo electrónico , a menos que ...



Habilite el factor de autenticación Google 2 paso por paso



Habilite el factor de autenticación Microsoft 2 paso por paso



Anderson

Available

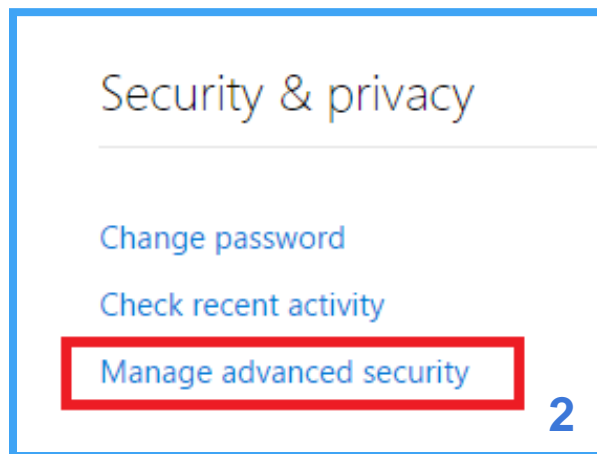
Invisible

Edit profile

Account settings

Sign out

1



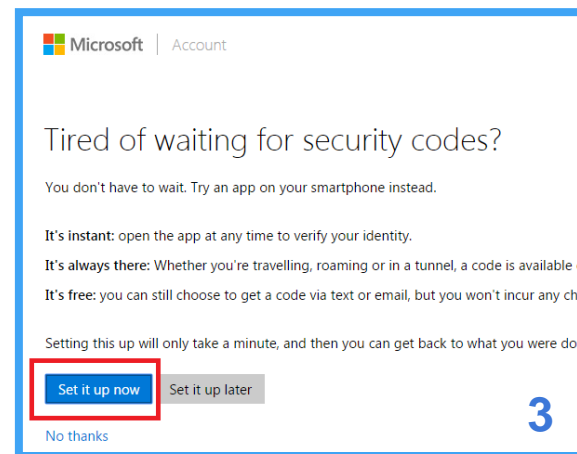
Security & privacy

Change password

Check recent activity

Manage advanced security

2



Microsoft | Account

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

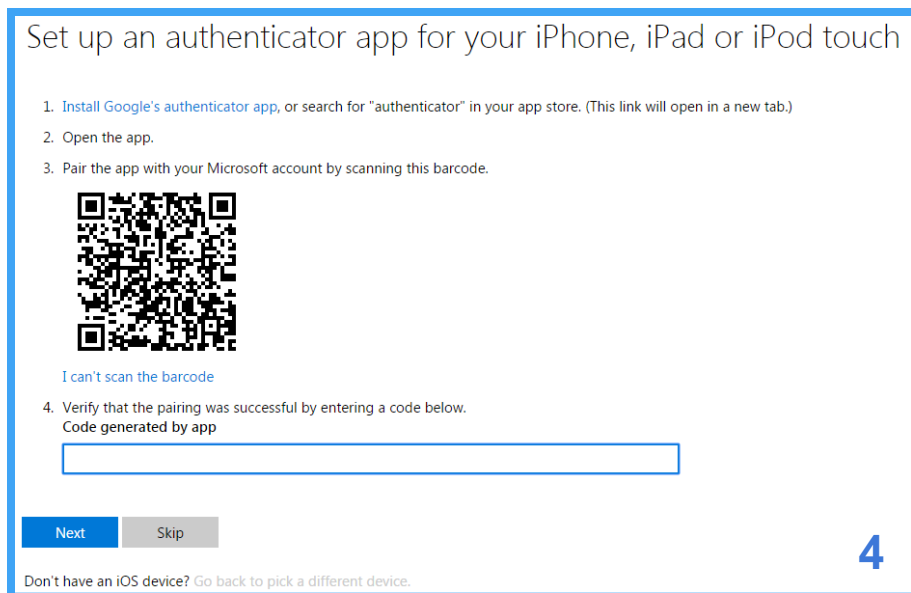
It's free: you can still choose to get a code via text or email, but you won't incur any ch

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

Set it up now Set it up later


No thanks

3



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

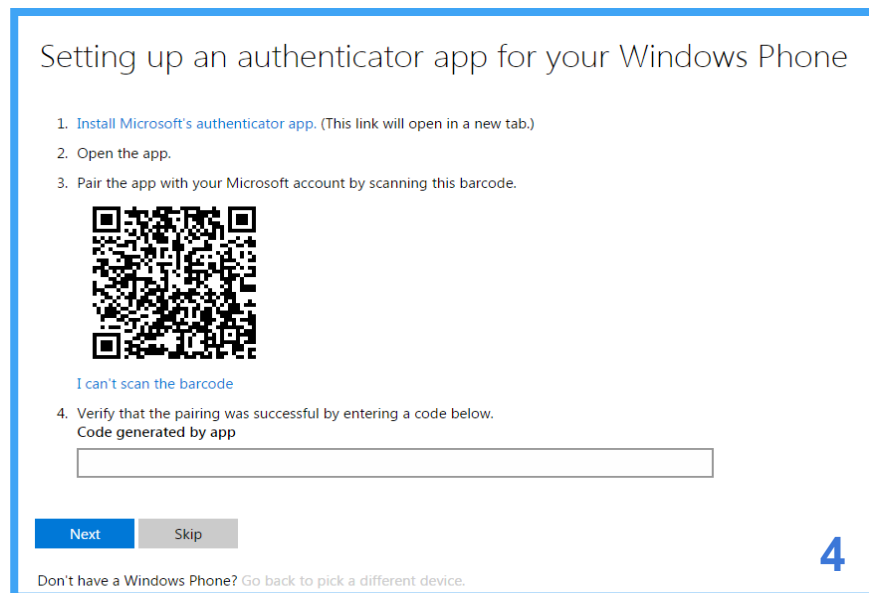
4. Verify that the pairing was successful by entering a code below.

Code generated by app

Next Skip


4

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

Next Skip

4

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

Computadoras de Hogar – Riesgos Prácticos



- Una computadora con varios usuarios
 - Diferentes tipos de acceso requieren diferentes niveles de seguridad;
 - Esta comprobado (piratería, los juegos and la pornografía) son frecuentemente usados por criminales para plantar virus y malware.
 - ¿Confía en la computadora de sus amigos? ¿Ellos cuidan su computadora de la misma manera que usted?
- Tenga cuidado sobre la conexión de dispositivos de almacenamiento o DVD de otras partes . infección por el virus a través de memorias USB sigue siendo una técnica muy común.

¿Como no poner su computadora en riesgo?

- [Divida negocios con diversión](#); no puede hacer ambos en el mismo equipo sin tomar riesgos serios. Lo mismo aplica en sus equipos móviles.
- [No comparta computadoras!](#) El error de uno, puede ser el problema de otro – esto incluye computadoras de salones de conferencia y computadoras de hoteles y cafés cibernéticos.
- [Compre una solución de seguridad completa](#)(Firewall, Antivirus, AntiSpam) y habilite OS (Windows, Android, Mac OSX, o Linux XYZ) y actualizaciones automáticas.
- [Evite](#) descargar o obtener software de [Fuentes Desconocidas](#) o compartidas por amigos.
- [Siempre mantenga el software de su computadora al corriente](#) lo que instalara la actualización de antivirus y paches.

Seguridad Cibernética
Esta en sus Manos!
Empiece Hoy.



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