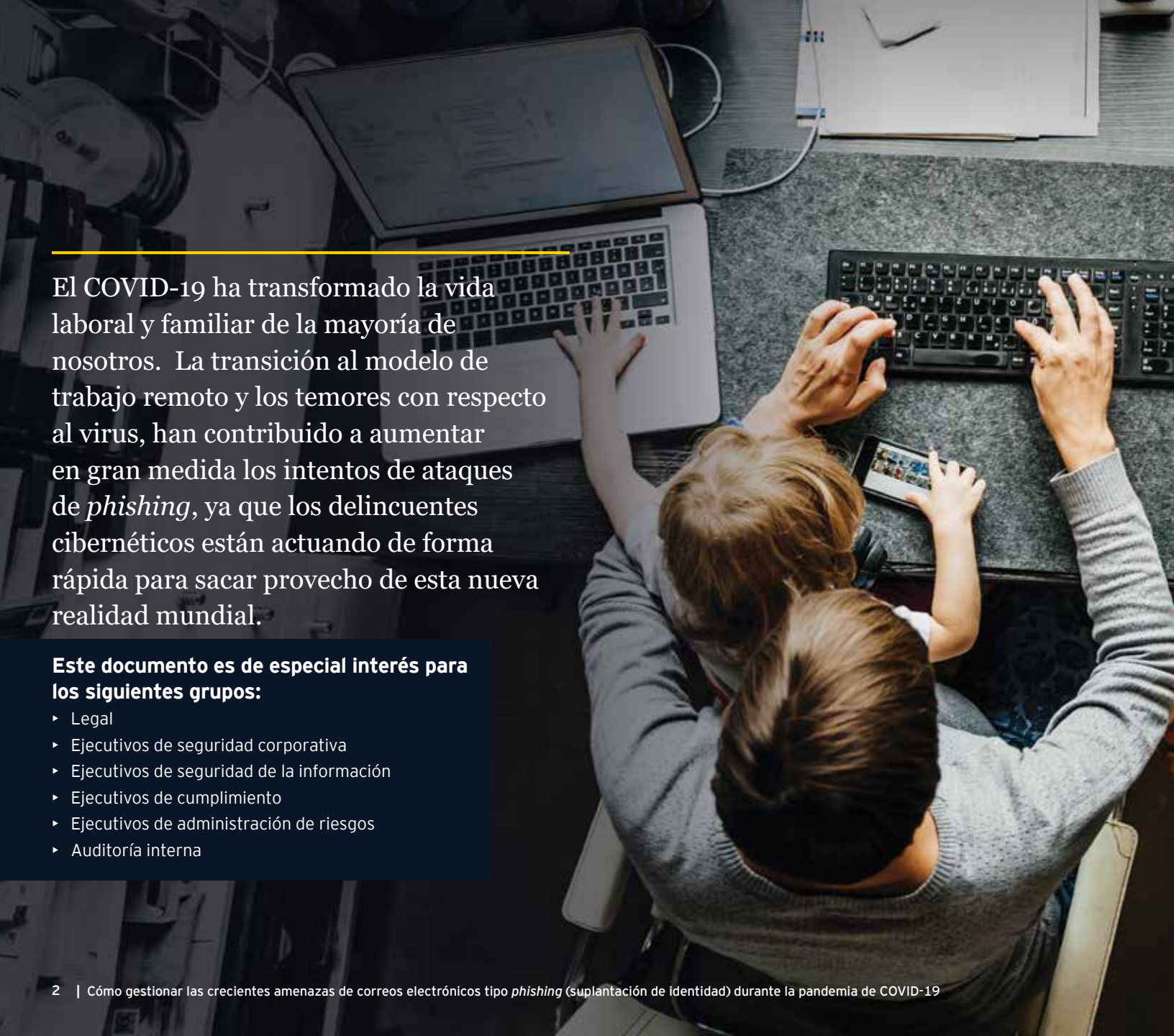
# ¡Ese correo también podría estar infectado!

Cómo gestionar las crecientes amenazas de correos electrónicos tipo *phishing* (suplantación de identidad) durante la pandemia de COVID-19

**Series ejecutivas para las áreas Legal, Cumplimiento y Tecnología**

EY

Building a better working world



El COVID-19 ha transformado la vida laboral y familiar de la mayoría de nosotros. La transición al modelo de trabajo remoto y los temores con respecto al virus, han contribuido a aumentar en gran medida los intentos de ataques de *phishing*, ya que los delincuentes cibernéticos están actuando de forma rápida para sacar provecho de esta nueva realidad mundial.

**Este documento es de especial interés para los siguientes grupos:**

- Legal
- Ejecutivos de seguridad corporativa
- Ejecutivos de seguridad de la información
- Ejecutivos de cumplimiento
- Ejecutivos de administración de riesgos
- Auditoría interna

# Los estafadores toman ventaja de la pandemia de COVID-19

Durante mucho tiempo, los correos electrónicos de fraude o tipo ***phishing*** han sido uno de los métodos más populares y efectivos utilizados por los delincuentes cibernéticos. Estos correos pueden utilizarse para distribuir información falsa, obtener alguna ganancia financiera de manera ilícita y conseguir información personal o confidencial de alguna víctima.

Los empleados que son víctimas de estos ataques pueden exponer la información vital de la compañía, que se encuentra almacenada no solo en su propia computadora, sino también en toda la red.

Actualmente, los delincuentes cibernéticos se aprovechan de la emergencia sanitaria a causa del COVID-19 para engañar a las personas que se sienten preocupadas a consecuencia de la pandemia. Los estafadores están enviando correos electrónicos que aparentan provenir de organizaciones legítimas como la Organización Mundial de la Salud, Instituciones de atención médica y entidades gubernamentales.

Casi todos los correos fraudulentos le piden al destinatario que haga clic en algún enlace o que abra algún archivo adjunto. Cualquiera de estas acciones podría ocasionar la activación de un software malicioso o podría redireccionar al usuario a un sitio que le solicite ingresar información confidencial.

## Además de las estafas relacionadas con el COVID-19, otros fraudes comunes son los siguientes:

- **Fraude contable:** una solicitud aparentemente enviada por algún departamento contable o financiero para que se apruebe el pago de una factura, el registro de una partida individual u otras transacciones financieras.
- **Redireccionamiento a sitios de redes sociales:** una notificación en redes sociales como una solicitud de amistad o una publicación que requiera que el usuario haga clic en algún enlace para acceder a ella.
- **Notificación de entrega de paquetes:** Un paquete que requiera que el destinatario de clic en algún enlace para confirmar la entrega o revisar el seguimiento del mismo.
- **Redireccionamiento de cuentas para compras en línea:** su cuenta de compras en línea (p. ej., Amazon o Apple) indica que hubo un acceso sospechoso, por lo que requiere que el usuario de clic en algún enlace para revisar o confirmar la compra.
- **Restablecimiento de contraseña:** su cuenta en alguna red social (p. ej., Facebook o Instagram) se ha visto comprometida, por lo que se requiere que el usuario haga clic en un enlace para volver a acceder a su cuenta.

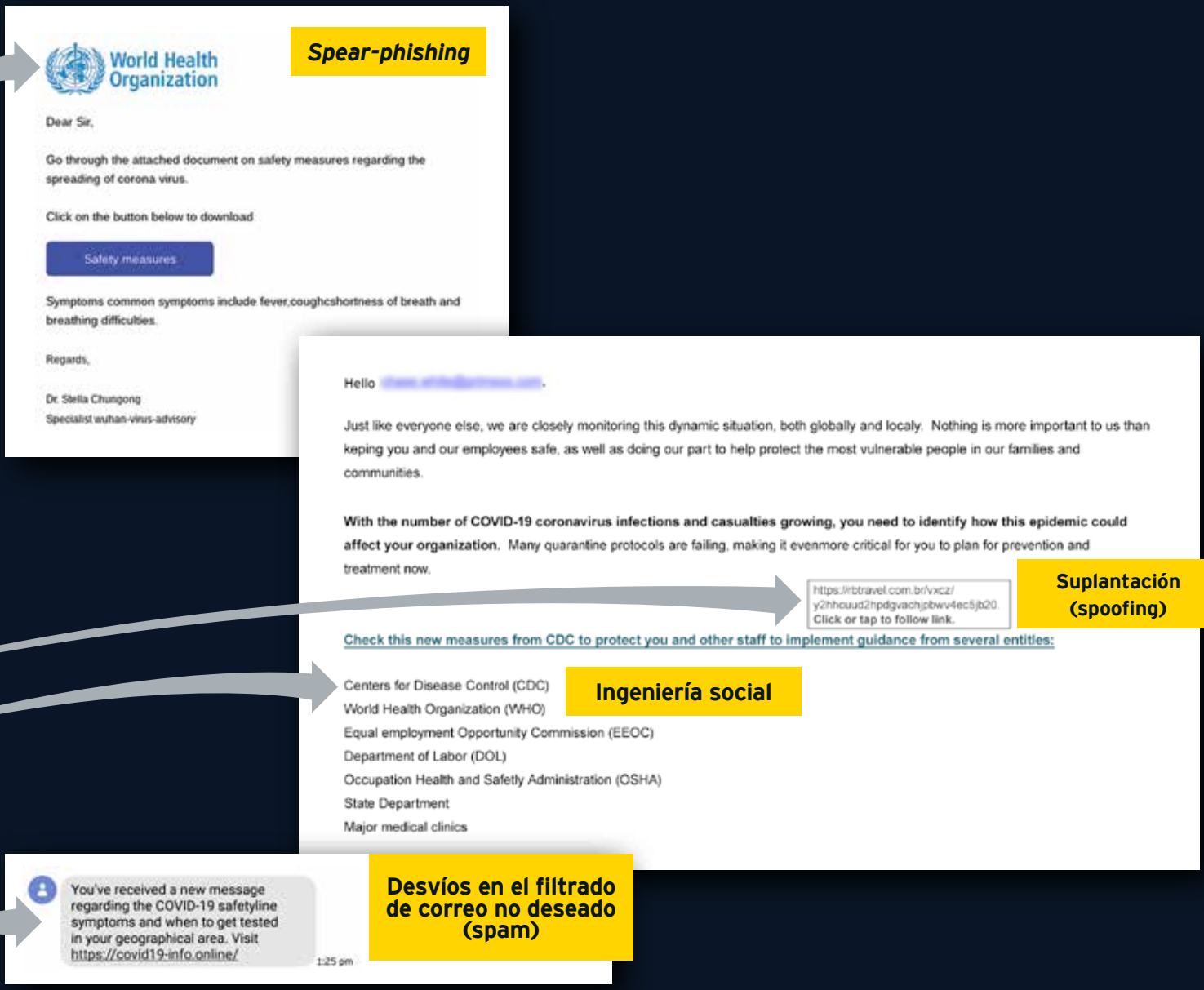
# Formas comunes de ataques de *phishing*

Como con la mayoría de los ataques de *phishing*, los delincuentes por lo general utilizan contenido legítimo obtenido de organizaciones prestigiosas para incitar al lector a hacer clic en algún enlace. La URL aparentemente pertenece a un sitio web legítimo, pero al hacer clic en ella, infecta la computadora de las víctimas redireccionándolas a un sitio malicioso que extrae sus datos.

Los ataques de *phishing* también se aprovechan de la necesidad de información en tiempos de crisis al enviar archivos adjuntos a los destinatarios, los cuales dicen contener información sanitaria importante. Cuando la víctima hace clic en el documento, sin saberlo podría estar otorgándole el control de su computadora a alguien más, que trabaja de forma remota a través de un código oculto.

Existen diversas formas que los delincuentes han estado utilizando para realizar los ataques de *phishing*, algunas de las más comunes son las siguientes:

- ***Spear-phishing:*** correos electrónicos falsos que aparentemente provienen de un remitente confiable y que les solicitan a las víctimas que revelen información confidencial o que abran enlaces que llevan a sitios web en donde deben ingresar sus credenciales de acceso.
- **Suplantación (spoofing):** utilizan nombres parecidos a los del personal de alto perfil dentro de las organizaciones, agregan o cambian los dominios para llevar a sitios maliciosos o utilizan formatos similares a los de ciertos sitios o correos electrónicos.
- **Ingeniería social:** utilizan LinkedIn y otra información de dominio público para planear jerarquías corporativas y utilizan esa información para perpetrar ataques de redireccionamiento con información fidedigna.
- **Desvíos en el filtrado de correo no deseado (spam):** utilizan tácticas como, por ejemplo, poner el texto del correo en tamaño cero, para desviar cualquier posible filtro de correo no deseado. Esto se considera un redireccionamiento más avanzado.


World Health Organization
Spear-phishing
Dear Sir,
Go through the attached document on safety measures regarding the spreading of corona virus.
Click on the button below to download
Safety measures
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.
Regards,
Dr. Stella Chungong
Specialist wuhan-virus-advisory
Hello
Just like everyone else, we are closely monitoring this dynamic situation, both globally and localy. Nothing is more important to us than keping you and our employees safe, as well as doing our part to help protect the most vulnerable people in our families and communities.
With the number of COVID-19 coronavirus infections and casualties growing, you need to identify how this epidemic could affect your organization. Many quarantine protocols are failing, making it evenmore critical for you to plan for prevention and treatment now.
https://rbtravel.com.br/vxcz/
y2hhouud2hpdgvachjzbwv4ec5jb20.
Click or tap to follow link.
Suplantación (spoofing)
Check this new measures from CDC to protect you and other staff to implement guidance from several entities:
Centers for Disease Control (CDC)
World Health Organization (WHO)
Equal employment Opportunity Commission (EEOC)
Department of Labor (DOL)
Occupation Health and Safetly Administration (OSHA)
State Department
Major medical clinics
Ingeniería social
You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/
1:25 pm
Desvíos en el filtrado de correo no deseado (spam)

# La transición al esquema de trabajo remoto supone distintos riesgos de ataques de *phishing*

Evidentemente, el *phishing* no es algo nuevo, pero los expertos en seguridad han reportado un incremento en los ataques de este tipo debido a la pandemia de COVID-19. Conforme acatemos las medidas de distanciamiento social y pasemos más tiempo trabajando de manera remota, el riesgo de caer en las trampas del *phishing* es cada vez mayor. Muchas interacciones que anteriormente se realizaban en persona, se han tenido que llevar a cabo a través de medios electrónicos y es posible que los empleados que trabajen de forma remota utilicen sus laptops corporativas para realizar tareas ajenas a la empresa. Los empleados que abren sus cuentas de correo electrónico personales desde sus laptops corporativas pueden caer en sitios infectados que roben la información confidencial de la empresa.

> “Un investigador en materia de seguridad, quien en línea aparece bajo el pseudónimo de DustyFresh, comenzó a rastrear algunos de estos dominios la semana pasada. De acuerdo a la lista que el investigador compartió en línea, estos delincuentes crearon más de 3,600 dominios nuevos que contienen el término “coronavirus” entre el 14 y el 18 de marzo.[1]

Las organizaciones han tenido que lidiar por mucho tiempo con las amenazas de correos electrónicos tipo ***phishing*** en los que el remitente se hace pasar por un colega o un gerente. Es posible que reciba un correo electrónico que aparentemente haya sido enviado por un colega y en el cual le pida que siga ciertas instrucciones para “hacer una transferencia”, “enviar datos financieros” u “otorgar acceso a la información confidencial de algún producto”. En el pasado, probablemente hubiera confirmado esta información con su compañero de al lado, pero, al no ser esta una opción actualmente, es posible que haga clic en el enlace de manera automática. A medida que los empleados pierden contacto personal, el riesgo de caer en estos ataques se incrementa de manera exponencial.

[1] Fuente: https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

## Para obtener más información, visite nuestro sitio web:

**ey.com/es_mx/assurance/privacy-cyber-response**

## Si nos mantenemos alerta, podemos evitar los ataques de *phishing*

- Siga las medidas de seguridad de su empresa con respecto a correos sospechosos enviados a su dirección de correo electrónico corporativa. Por ejemplo, muchas empresas cuentan con herramientas que permiten marcar de forma inmediata cualquier correo electrónico que no pueda ser verificado fácilmente.
- Revise los lineamientos de ciberseguridad de su empresa y tome los cursos correspondientes.
- Siempre que sea posible, utilice las herramientas corporativas internas seguras, como la mensajería instantánea y los sitios de colaboración, en lugar del correo electrónico. Si no está familiarizado con estas herramientas, ahora es el momento de que las adopte.
- Verifique la dirección de correo electrónico del remitente para asegurarse de que el nombre del dominio sea correcto. Por ejemplo, ***real.employee@acme.com*** no es lo mismo que ***realemployee@acmee.com***.
- Tenga cuidado con los correos electrónicos genéricos que no están dirigidos específicamente a usted.
- Cuestione la autenticidad de cualquier correo que tenga errores gramaticales y de redacción.
- La mayoría de los programas de correo electrónico (p. ej., Microsoft Outlook) le alertarán sobre cualquier correo sospechoso. No ignore estas advertencias.
- Utilice la mensajería instantánea o llame por teléfono al colega que aparentemente es el remitente del correo sospechoso.
- Tenga cuidado con cualquier instrucción le solicite descargar un archivo como una factura o un estado de cuenta.
- Cuando el correo le solicite hacer clic en una URL, verifique la dirección para determinar si lo redirige a un sitio web conocido. No haga clic en ningún enlace a menos que pueda verificarlo.
- No realice ninguna acción que se encuentre fuera de los flujos de trabajo estándar sin antes verificar la información (p. ej., transferir dinero para procesar pagos).
- No responda a ningún correo electrónico que le solicite información personal. Cualquier organización legítima que le solicite esta información de carácter confidencial, le enviará un enlace seguro que encripte los datos.
- No abra ningún archivo adjunto sin antes verificarlo. Póngase en contacto con el remitente por teléfono, o utilice alguna otra herramienta de comunicación interna segura para confirmar la autenticidad de los documentos antes de abrirlos.

**EY** | Aseguramiento | Asesoría de Negocios | Fiscal-Legal | Fusiones y Adquisiciones

Acerca de EY

EY es líder global en servicios de aseguramiento, asesoría, impuestos y transacciones. Las perspectivas y los servicios de calidad que entregamos ayudan a generar confianza y seguridad en los mercados de capital y en las economías de todo el mundo. Desarrollamos líderes extraordinarios que se unen para cumplir nuestras promesas a todas las partes interesadas. Al hacerlo, jugamos un papel fundamental en construir un mejor entorno de negocios para nuestra gente, clientes y comunidades.

Para mayor información visite **www.ey.com/mx**



**ey.com**




**/EYMexico**


**/EYMexicoOficial**


**@EYMexico**


**company/ernstandyoung**

## Contactos:

**Ignacio Cortés**
Forensic & Integrity Services
Leader, EY Latin America North
ignacio.cortes.Castan@mx.ey.com

**Juan Ramírez**
Forensic & Integrity Services - Forensic Technology and Cyber Response Senior Manager, EY México
juan.ramirezVald@mx.ey.com

**Derick Vasquez**
Forensic & Integrity Services - Forensic Technology and Cyber Response Manager, EY México
derick.vasquez@mx.ey.com