WatchGuard

NO ESPERE A QUE SEA DEMASIADO TARDE.

AGREGUE SEGURIDAD PARA MANTENER LA VERDADERA IDENTIDAD.

Está a Solo Una Contraseña Débil de…

… Incluso sus contraseñas "complicadas" se pueden descifrar.
Ya no quedan dudas de que las contraseñas no son suficientes para mantener la seguridad de sus activos, cuentas e información.

Estos son algunos de los motivos:

74% de las vulnerabilidades en 2022 involucraron al elemento humano, incluido el robo de credenciales[1]

51% de las personas utilizan la misma contraseña para cuentas laborales y personales[2]

Por último, las personas eligen **contraseñas débiles**

WatchGuard

Este es un listado de las 20 contraseñas más comunes encontradas en la dark web[3], debido a vulneraciones de datos:

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

WatchGuard

No es Difícil que las Contraseñas Caigan en Manos Equivocadas

Se puede adquirir un conjunto de credenciales completo en la dark web por USD 8 a 25,[4] lo que permite vulnerar sistemas con más facilidad y a un menor costo. Si eso no funciona, un criminal cibernético habilidoso podría descifrar las contraseñas de la mayoría de las personas en el tiempo que a usted le lleva leer el listado de contraseñas de la página anterior.[5]

Las contraseñas son fáciles de robar y solo proporcionan una línea de defensa. Por lo general, si un hacker logra robar la contraseña de un solo empleado, obtiene acceso a toda la red. Una vez adentro, puede hacer lo que quiere. Generalmente, esto se reduce a propagar malware o robar, modificar o eliminar información crítica.

WatchGuard

Robar Su Contraseña Es Fácil

El proceso de robar una contraseña es alarmantemente sencillo (y redituable) para los hackers. Las herramientas y tecnologías que usan para adivinar las contraseñas son cada vez más sofisticadas y están automatizadas hasta el punto en que el proceso manual de "adivinar" las contraseñas ya no es necesario. Incluso cuando lo es, los algoritmos avanzados, la ingeniería social (por ejemplo, los ataques de suplantación de identidad o los troyanos), los registradores de teclas y otros métodos les permiten adivinar eficientemente y probar las contraseñas más probables, lo que muchas veces tiene éxito.

Entre los métodos para deducir contraseñas más comunes, se encuentran:

Ataque de Diccionario

Los hackers intentan adivinar una contraseña escribiendo una lista común de palabras de un diccionario de contraseñas. Los diccionarios de contraseñas más avanzados incluyen listas de las palabras más comunes usadas en contraseñas. Este es un método relativamente simple, pero es eficaz para adivinar las contraseñas menos complejas. Si usted usa palabras reales en cualquiera de sus contraseñas, sus credenciales están en riesgo.

Ataque de Fuerza Bruta

Aunque no es tan eficiente como el ataque de diccionario, con el tiempo, un ataque de fuerza bruta adivina con más eficacia las contraseñas. Con este método, los hackers usan herramientas para probar repetidamente cualquier combinación posible de letras, números y símbolos en una contraseña hasta que logran descifrarla. Un enfoque similar es un ataque de fuerza bruta inversa, en el que el hacker prueba una contraseña en muchos nombres de usuario.

Ataque de Arcoíris

Este método usa un recurso llamado tabla de arcoíris para descifrar valores de hash de contraseñas (básicamente contraseñas mezcladas que están almacenadas en bases de datos de sistemas) de una manera mucho más eficiente y eficaz que los ataques de fuerza bruta y de diccionario.

WatchGuard

Ataque de Relleno de Credenciales

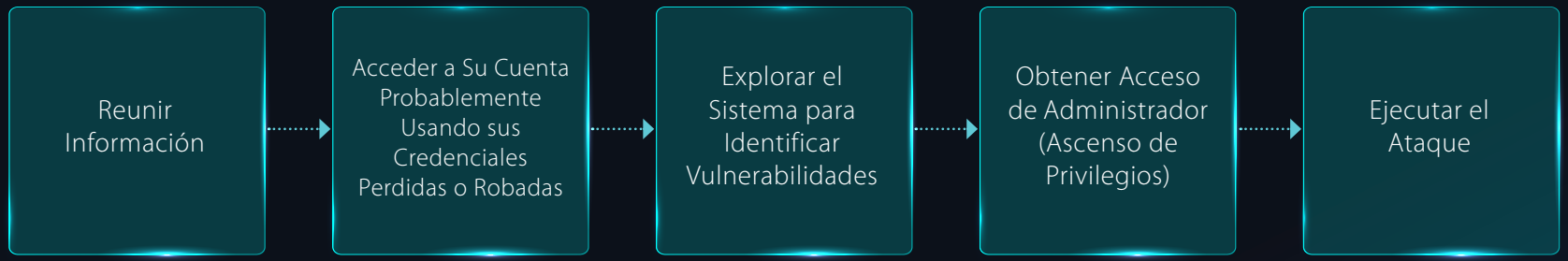
Como muchas personas usan las mismas contraseñas o variaciones de ellas en diferentes cuentas, los hackers encontraron una manera de contrastar automáticamente listas de bases de datos de combinaciones de usuarios y contraseñas filtradas con el inicio de sesión del sitio web objetivo. Según Shape Security, el 90% de los intentos de inicio de sesión de los vendedores minoristas en línea son de este tipo de ataque y este método es eficaz para los hackers alrededor del 3% de las veces.

Ingeniería Social

Este enfoque tiene una variedad de estilos, todos asociados con la idea de engañar o manipular a las personas para que divulguen su información o realicen cierta acción. Los métodos comunes de ingeniería social que se usan para robar contraseñas incluyen la suplantación de la entidad y el uso de troyanos. Un enfoque menos común es "mirar por encima del hombro", en el que el hacker simplemente mira cuando el usuario escribe su contraseña.

Debido a la cada vez mayor sofisticación de las tecnologías y herramientas de los hackers, descifrar la contraseña es el paso más fácil de un ataque. De hecho, es tan fácil que muchas veces ni siquiera les implica adivinar. Lo más aterrador es que sin importar qué tan segura sea la contraseña, todo lo que hace falta es una contraseña débil de un colega para que todo el sistema de su empresa tenga riesgo de infiltración.

Las credenciales perdidas o robadas otorgan ganancias a los hackers porque permiten el robo de datos o el acceso a sus sistemas laborales, donde se pueden ejecutar el ransomware u otros ataques de malware provechosos. Los expertos en seguridad informática y el hacker de sombrero blanco Roger Grimes describen este proceso en su libro titulado *Hackear al Hacker (Hacking the Hacker)*.



Según Grimes:

> Si el hacker hizo los deberes en la etapa de huellas digitales, entonces esta etapa no es para nada difícil.

Es decir, para los hackers es muy fácil acceder a las cuentas de otras personas. Algunos, además, cubren sus pasos o crean una puerta de entrada para acceder en el futuro, aunque esto no siempre es así.

¿Cómo nos aseguramos de que la persona que ingresa la contraseña sea realmente quien dice ser? ¿Cómo puede mantener su verdadera identidad?

Los expertos en agencias gubernamentales e independientes de todo el mundo ofrecen sabios consejos sobre proteger los sistemas empresariales de los ataques. Una alerta reciente de las autoridades en ciberseguridad de los EE. UU., Nueva Zelanda, Canadá, Países Bajos y el Reino Unido concluyó que utilizar una MFA y políticas de contraseñas sólidas para fortalecer las credenciales son las mejores prácticas contra el crecimiento de los ciberataques.[6] Y no se trata de cualquier tipo de protección de identidad y credenciales, ya que los criminales cada vez son más sofisticados, por lo que así deben ser nuestras soluciones de seguridad. Como ejemplo, en agosto de 2021, la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) agregó la autenticación de un solo factor a su lista de Malas Prácticas de Ciberseguridad[7] —un claro mensaje a todas las organizaciones que se apoyan únicamente en contraseñas como protección—.

Muchas Organizaciones Han Intentado Cambiar el Comportamiento de los Empleados en Relación con las Contraseñas

Un método para mitigar el riesgo de que se robe una contraseña es entrenar a sus empleados para que creen contraseñas más fuertes y las cambien con mayor frecuencia. Sin embargo, cambiar el comportamiento de todos los empleados no solo es desafiante, también es poco eficaz.

Históricamente, este enfoque no funciona

Como evidencia, tenemos a millones de empresas que han sufrido el robo de sus bases de datos y decenas de millones de contraseñas que se han filtrado y que están disponibles en línea (nótese que uno puede comprar muchas de estas credenciales en la dark web).

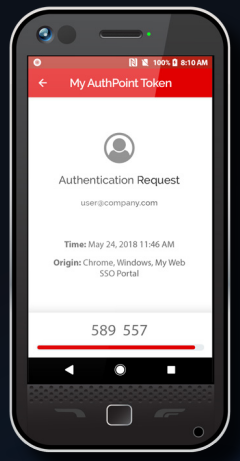
Crea una experiencia del usuario muy compleja

Usar contraseñas únicas, totalmente aleatorias y de 16 caracteres en todas las cuentas es muy complejo. El motivo por el que las personas usan contraseñas simples es porque no es fácil recordar las contraseñas. Muchas personas crean contraseñas un poco más complejas, pero para compensar la complicación, usan la misma contraseña (o variaciones de esta) en diferentes cuentas.

Ya que las contraseñas no son suficientes, ¿hay algo que lo sea?

La autenticación multifactor (MFA) es un método de verificación que agrega un nivel de seguridad a los inicios de sesión más allá de un simple nombre de usuario y contraseña. Ayuda a asegurarse de que los hackers no puedan acceder a sus sistemas, incluso si se filtra la contraseña de uno de sus empleados. Específicamente, se prefiere un enfoque multifactor por sobre una autenticación de un solo factor porque incluye:

- **Algo que tiene** *(token, teléfono móvil)*
- **Algo que conoce** *(contraseña, PIN)*
- **Algo que eres** *(huella digital, rostro)*



WatchGuard

Nota de Precaución: No todas las Soluciones de MFA se han Creado Iguales

La autenticación multifactor basada en SMS ya no es un método seguro y de confianza. Los usuarios con autenticación basada en SMS deberían migrar a otros métodos inmediatamente. En las pautas sobre la identidad digital de 2016, el Instituto Nacional de Estándares y Tecnología (NIST) alentó a los usuarios a apartarse de la autenticación basada en SMS:

"Debido al riesgo de que los mensajes SMS puedan interceptarse o redireccionarse, quienes implementen sistemas nuevos deberán considerar cuidadosamente el uso de autenticadores alternativos. La autenticación fuera de banda que usa [SMS o voz] es obsoleta y se está considerando su eliminación en futuras ediciones de estas pautas".

Harvard Business Review fue más allá y declaró: "Podría decirse que la autenticación basada en SMS se ha convertido en un vector de ataques más que en una medida de seguridad".

El motivo por el que la autenticación basada en SMS es riesgosa es que los mensajes de texto son vulnerables a las intercepciones. Reddit fue una víctima notable de esto en 2018. Reddit publicó un comentario acerca del ataque en su propio sitio y lo atribuyó a la debilidad de la autenticación basada en SMS: "Aprendimos que la autenticación basada en SMS es mucho menos segura de lo que esperábamos, y el ataque principal fue por intercepción de SMS. Recalcamos esto para alentar a todos a migrar a la 2FA basada en tokens".

Si bien usar la MFA basada en SMS es mejor que depender solo de una contraseña y un nombre de usuario, de todos modos los usuarios siguen siendo vulnerables a los ataques. Para mitigar el riesgo, las empresas deberían depender de una solución de MFA que solo use métodos fuertes de autenticación.

WatchGuard

¡Proteger la Contraseña También es Importante!

Si bien la MFA por sí sola ayuda bastante, se sigue considerando a las contraseñas para la validación de identidad, que es el motivo por el que los expertos en ciberseguridad también recomiendan robustecer y controlar las credenciales adicionales. En particular, un producto de administración de contraseñas a nivel empresarial es una propuesta beneficiosa para ambas partes en muchas empresas. No solo promueve el uso de contraseñas únicas y complejas, sino que proporciona a los usuarios una herramienta para que puedan acceder y recuperar esas contraseñas de forma fácil y segura cuando sea necesario. Y lo que es mejor, el administrador de contraseñas y MFA pueden implementarse y administrarse juntos, y así formar una solución eficaz hecha para los requisitos específicos de los negocios.

Dado el fuerte comercio de credenciales perdidas/robadas en la dark web, un servicio de monitoreo también puede ofrecer a las empresas tiempo valioso para estar alertas a un conjunto de credenciales vulneradas de su dominio, antes de que puedan utilizarse en un ataque dañino.

WatchGuard ofrece una solución de autenticación multifactor fácil de utilizar con un administrador de contraseñas corporativo y un servicio de monitoreo de la dark web en nuestro paquete AuthPoint Total Identity Security.

WatchGuard®

¿Cómo ayuda AuthPoint Total Identity Security?

MFA de AuthPoint es un servicio de autenticación multifactor (MFA) que ayuda a las empresas a mantener la seguridad de sus activos, información e identidades de usuarios. Esta solución les solicita a los usuarios que usen más de dos factores de autenticación para iniciar sesión, en lugar de depender solo de una contraseña. Además, AuthPoint Total Identity Security incluye nuestro servicio de administrador de contraseñas corporativas y de monitoreo de la dark web. Beneficios clave:

Múltiples capas de autenticación

Las empresas pueden reducir significativamente el riesgo de que se roben sus cuentas. Si un hacker obtiene la contraseña de un empleado, sigue habiendo otra capa de seguridad para ayudar a evitar el ataque.

Usuarios felices y adopción simple

Los usuarios aprueban o rechazan el inicio de sesión con un simple toque en la aplicación móvil de AuthPoint. Una vez que iniciaron sesión, los usuarios pueden disfrutar de un inicio de sesión único (SSO) para acceso rápido a sus aplicaciones y entornos.

Y lo que es mejor, el Administrador de Contraseñas Corporativas está disponible desde la aplicación AuthPoint y puede utilizarse tanto con las contraseñas corporativas como con las personales.

Administración desde WatchGuard Cloud – Una interfaz de fácil administración

Los productos AuthPoint Total Identity Security son administrados totalmente en la nube. Esto significa que no hay hardware costoso para implementar y no es necesario actualizar software.

Una solución creada para empresas

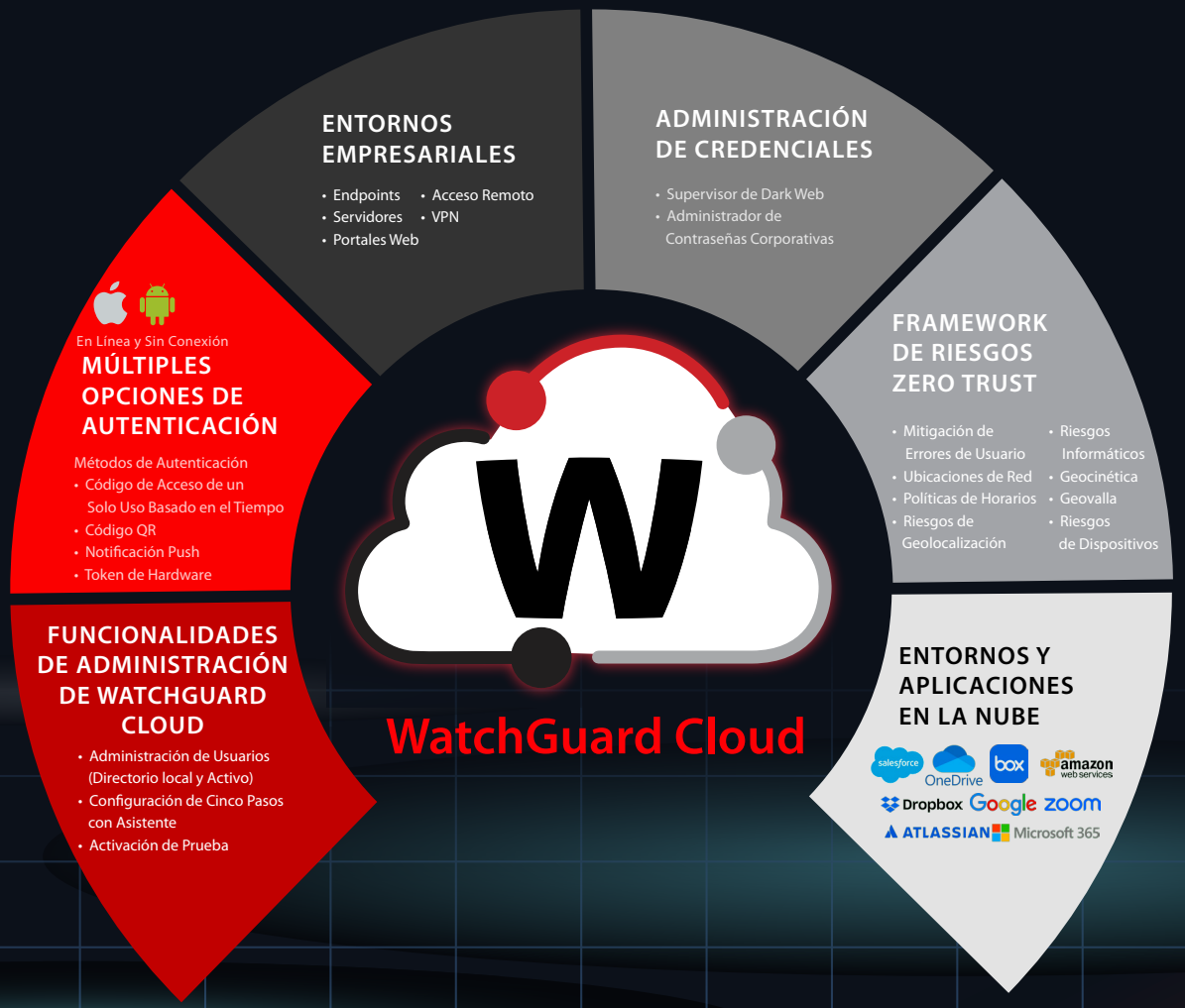
A diferencia de la 2FA y de los administradores de contraseñas hechos para uso del consumidor, AuthPoint se diseñó para abordar casos de uso corporativos. Por ejemplo, autentica a los usuarios de Windows/macOS tanto en línea como sin conexión a Internet, por lo que pueden iniciar sesión de forma segura incluso si quieren acceder a su cuenta desde un avión.

Ofrece una protección poderosa por menos de lo que cuesta su café de la mañana.

¿Apostaría su empresa a la seguridad de la contraseña de cada uno de sus empleados? Mantenga la Verdadera Identidad con AuthPoint. Es asequible, potente y fácil de usar.

WatchGuard

Mantenga la Verdadera Identidad con WatchGuard AuthPoint.

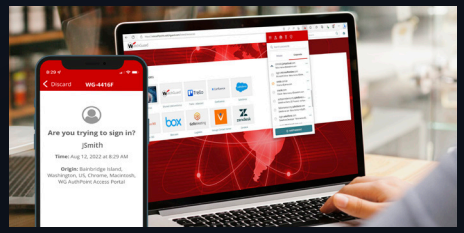


WatchGuard

Portafolio de WatchGuard

Seguridad de Red

WatchGuard ofrece una gran variedad de soluciones de seguridad de red, que incluyen desde dispositivos de escritorio y dispositivos montados en rack de 1 unidad, hasta firewalls virtuales y en la nube. Nuestros dispositivos Firebox® ofrecen servicios de seguridad críticos, desde servicios de prevención de intrusiones estándar, filtrado de URL, Gateway AV, control de aplicaciones y filtro de correo no deseado, hasta protecciones avanzadas como sandboxing de archivos, filtrado de DNS, entre otros. La inspección detallada de paquetes (DPI) de alto rendimiento le permite aprovechar todos nuestros servicios de seguridad contra ataques que intentan ocultarse en canales cifrados como HTTPS. Además, cada dispositivo Firebox ofrece SD-WAN listo para usar que mejora la resiliencia y el rendimiento de la red.

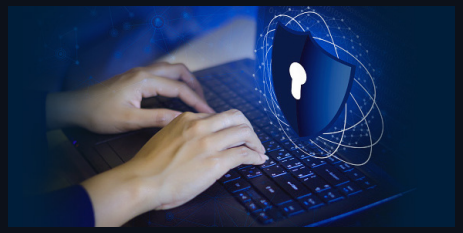


Identity Security y MFA

WatchGuard AuthPoint® es la solución correcta para abordar la brecha de seguridad basada en contraseñas con la autenticación multifactor en una plataforma de nube fácil de usar. El enfoque exclusivo de WatchGuard agrega el "ADN del teléfono móvil" como factor de identificación para garantizar que solo las personas correctas tengan acceso a las redes confidenciales y a las aplicaciones en la nube. AuthPoint también ofrece una experiencia de usuario optimizada con métodos de autenticación en línea y sin conexión, además de un portal de aplicación web para un fácil acceso mediante inicio de sesión único.

Wi-Fi Seguro en la Nube

Wi-Fi Seguro en la Nube: las soluciones de Wi-Fi seguro, administradas en la nube de WatchGuard, proporcionan un espacio aéreo seguro y protegido para entornos Wi-Fi, al tiempo que eliminan los dolores de cabeza administrativos y reducen en gran medida los costos. WatchGuard ofrece tecnología Wi-Fi 6 con cifrado WPA3 seguro para todos los entornos, desde oficinas en el hogar hasta campus corporativos expansivos. Con WatchGuard Cloud, la configuración y la administración de políticas de la red Wi-Fi, la implementación sin intervención, los portales cautivos personalizados, la configuración de VPN, las herramientas de participación expansiva, la visibilidad de los análisis de negocios y las actualizaciones están a solo un clic de distancia.



Seguridad de Endpoints

Las soluciones de Seguridad de Endpoints de WatchGuard lo ayudan a proteger los dispositivos contra las ciberamenazas. WatchGuard EPDR y Advanced EPDR, nuestras soluciones emblemáticas de seguridad de endpoints, impulsadas por IA, le permiten mejorar su posición de seguridad, ya que integran sin inconvenientes la protección de endpoints (EPP) y las capacidades de detección y respuesta (EDR) con nuestros servicios de Threat Hunting y de Zero Trust Application. Todas estas soluciones están estrechamente integradas dentro de WatchGuard Cloud y ThreatSync, que proporcionan una visibilidad y una inteligencia valiosas, al tiempo que fortalecen la detección y respuesta de productos cruzados (XDR).

Referencias:

1. https://www.verizon.com/business/resources/reports/dbir/
2. https://www.spiceworks.com/it-security/identity-access-management/news/world-password-day-2022/)
3. https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html
4. https://www.securitymagazine.com/articles/94405-a-look-into-the-pricing-of-stolen-identities-for-sale-on-dark-web
5. https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity
6. https://www.cisa.gov/uscert/ncas/alerts/aa22-137a
7. https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en ciberseguridad unificada. Nuestra Unified Security Platform® está diseñada exclusivamente para que los proveedores de servicios administrados brinden seguridad de primer nivel que aumente la escala y la velocidad de su negocio al mismo tiempo que mejore la eficiencia operativa. Con la confianza de más de 17 000 revendedores de seguridad y proveedores de servicios para proteger a más de 250 000 clientes, los productos y servicios galardonados de la empresa abarcan seguridad e inteligencia de red, protección avanzada de endpoints, autenticación multifactor y Wi-Fi seguro. Juntos, ofrecen cinco elementos que son vitales en una plataforma de seguridad: seguridad integral, conocimiento compartido, claridad y control, alineación operativa y automatización. La empresa tiene su oficina central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia-Pacífico y Latinoamérica. Para obtener más información, visite WatchGuard.com/es.

VENTAS EN MEXICO +52 55 5347-6063 **VENTAS ESPAÑA** +34 917 932 531 **SITIO WEB** www.watchguard.com/contact