Relleno de Credenciales

Deseas terminar con un mal hábito que posiblemente no quieres reconocer, inclusive si es uno de tus peores, no es el cigarrillo, la comida chatarra, la procastinación o comer uñas —es reutilizar credenciales de ingreso en sitios web. ¿Lo veías venir cierto?

Utilizar el mismo nombre de usuario y contraseña una y otra vez es un mal hábito que muchos de nosotros tenemos. Vamos a la segura — un apodo, el nombre de alguno de nuestros hijos, el nombre de un barco o una franquicia de deportes, algo que estemos seguros de recordar — Lo que sea, ¿cierto? ¿Qué tan perjudicial puede ser? En decenas de billones de dólares es dañino. Este único mal hábito es el responsable de las más grandes brechas de seguridad en internet.

La Naturaleza de Este Hábito

Mucho de lo que internet impulsa, hits de dopamina, un deseo, lo que pueda ser consumido a través de Amazon, suscribirse a un periódico o cualquier cosa que te emocione. Cuando queremos algo estamos en un estado de alto deseo y probablemente, también más lejos de escapar a cualquier acción resultante de un proceso de pensamiento que nos saque de un trance impulsivo. La última cosa en tu mente cuando estás ingresando a una subscripción online de Deportes Ilustrados cuando han hecho un reportaje sobre tu mariscal de campo favorito, es retrasar el proceso pensando en la seguridad, lo mismo cuando compras nuevos equipos de vanguardia para tu computadora de juegos o una vajilla para tu comedor.

Somos criaturas impulsivas, esclavos del estado de trance inducido por un deseo y la magia de la publicidad iniciada por la firma Madison Avenue y cuando estamos en este estado de trance, cometemos errores. Recuerda el viejo adagio romano *caveat emptor,* que se traduce comocomprador ten cuidado, has tus diligencias antes de comprar algo. En el uso de la era digital, también puede ser aplicado a compras seguras. No se apresure a comprar en línea, no permita que el impulso lo guíe. Elija un nombre de usuario seguro y una única contraseña. Tómese su tiempo, respire, piense, la oportunidad de compra no se va a ningún lugar, es solamente el deseo y el impulso hablando.

El Nuevo Caveat Emptor

Personas que pretenden capitalizar un impulso o adicción han estado aquí desde que existe la raza humana. Solía ser nada más una transacción de dos partes, vendedor y comprador, el segundo buscando obtener información y un mejor precio y el primero queriendo obtener el precio justo del mercado. La simple transacción de dos partes (comprador-vendedor) es nostalgia en internet, ahora hay muchas partes interesadas en sus compras en línea, no tienen que estar ahí en el momento de la compra, pueden aparecer mucho tiempo después de la transacción. La irrelevancia de tiempo es debido a particularidades de compras en línea. El pago es digital, va de su cuenta de banco, tarjeta de crédito Stripe, o PayPal a la cuenta del vendedor. Solamente hay que registrarse en el sitio web del vendedor con un nombre de usuario y contraseña los cuales son almacenados en el sitio web del vendedor y así es como una tercera parte entra en juego.

En la era digital no los ves, no están a tu lado, no te hacen conversación, están ocultos en el ciberespacio y capitalizarán de tu error días posteriores cuando ejecuten su negocio. El problema de reutilizar credenciales es tan endémico que un término de la industria de seguridad ha evolucionado para describir una empresa delictiva organizada, un relleno de credenciales o un ataque de relleno de credenciales.

Caveat emptor o Cuidado por parte del comprador no solamente aplica para proteger al comprador de vendedores engañosos, ahora hace una alianza entre comprador y vendedor para protegerlos de tercereas partes. Tu mal hábito es solamente parte del problema, la otra parte no es tu culpa, es culpa de la organización a la que le confiaste tus datos. En su defensa, los recursos aplicados en relación a su seguridad son enormes y deben operar veinticuatro horas al día toda la semana desde cada esquina del planeta. El espacio digital no puede ser geográficamente medido en kilómetros, eso debe ser evidente para cualquiera que haya tenido una llamada por Skype o una conferencia de Zoom con gente de otras partes del mundo.

Las Brechas

Deben de haber habido enormes brechas de seguridad en la última década. La más notable fue la de Yahoo en 2013, pero seguramente ha habido algunas otras también grandes. El pobre Yahoo ganó mala reputación por ser el primero con una masiva brecha de seguridad. La variante indú de Alibaba, llamada Aadhaar, tuvo una brecha de seguridad en enero de 2018 que le entregó a los hackers un tesoro de información que incluía nombres, direcciones, fotos, números de teléfono, emails y lo más escalofriante de todo, información biométrica como huellas digitales y escaneos de iris. Esto afectó alrededor de un billón de personas. Algo aún más interesante es cómo los malos actores ganaron acceso, lo hicieron a través de una base de datos gubernamental pública de India, asociada con una compañía de utilidad.

El mismo Alibaba fue golpeado en noviembre 2019. fue un trabajo interno, una manzana podrida en el departamento de desarrollo estaba trabajando para una compañía de marketing y había estado recopilando información de los clientes que incluía nombres de usuario y números de teléfono. Hizo esto con un software rastreador que él mismo escribió. El desarrollador y su empleado estaban recolectando datos para ellos mismos, nada se vendió en el mercado negro, los dos fueron tres años a la cárcel. LinkedIn, los datos de setecientos millones de usuarios fueron posteados en un oscuro fórum en junio de 2021. Esto impactó a más del noventa por ciento del uso básico de la aplicación de LinkedIn, fue pirateado con técnicas de raspado. LinkedIn le restó importancia como una violación de su contrato de servicio, pero sin consecuencias serias para sus usuarios. Su razón fundamental fue que no solicitan información sensible a los usuarios.

Eso fue cierto en el sentido de que no hubo números de cuentas de banco o inmediata información rentable que pudiese ser vendida en el mercado negro, pero estamos hablando de credencial de relleno, y tenían nombres de usuario y contraseñas. Lo que LinkedIn está minimizando es que los nombres de acceso y contraseñas de esos setecientos millones de usuarios probablemente permitió el acceso a un exponencial número de sitios web que tenían información sensible. Piensa en esto como si fuera una explosión nuclear. La onda electromagnética que viaja por kilómetros es efecto secundario de la información pirateada en todos los otros sitios web que van a ser pirateados en el futuro como resultado del relleno de credencial. En abril 2019 Facebook fue hackeado, esto afectó a más de quinientos treinta millones de usuarios. Esta brecha incluyó números de teléfono, nombres de cuentas y IDs de Facebook. La información fue posteada en línea dos años después. Esta es solamente una pincelada de la brecha de información que ha tenido lugar en la última década, no hay nada que puedas hacer para protegerte de las brechas de seguridad de las corporaciones, pero te puedes proteger contra ataques en otros perfiles online a través de buenos hábitos de nombres de usuario y contraseñas.

Las Vulnerabilidades

Los atacantes usan herramientas autónomas como [Selenium](https://www.selenium.dev/), un paquete de desarrollo de automatización del navegador, [cURL](https://curl.se/), un marco de transferencia de datos de código abierto, herramientas de diseño personalizado si el sofisma está ahí. Estas herramientas salen y simultáneamente automatizan los procesos de atentados de ingreso en miles de sitios. Si tienes el hábito de reutilizar nombres de usuario y contraseñas incrementas el chance de un golpe, puede ser tu cuenta de banco, tu cuenta de Google, con esto les das acceso a las contraseñas almacenadas en las páginas de Google Chrome, así obtendrán todo.

Los ataques de relleno de credenciales no son lo mismo que ataques de fuerza bruta. Solamente es de verificar en los servicios en línea las credenciales que tienen, una vez que obtienen tus datos salen del banco, luego las compras en línea inician, te despiertas un día y la mitad de tus ahorros se han ido, es una pesadilla, pregúntale a alguien que lo haya experimentado.

Las cinco industrias más vulnerables son las ventas al menudeo en línea y los e-commerce, servicios de video en directo como Netflix, servicios financieros y bancos, así como educación superior, esta última podría verse como fuera de lugar, pero así es, de hecho, la riqueza de información lo hace un objetivo de alto valor, de igual manera las organizaciones de asistencia médica.

La Solución

Siempre debes protegerte de ataques de relleno de credencial. La defensa más importante es romper con el hábito de contraseñas y nombres de usuario vagos y la repetición de los mismos, pero esto solamente te cubre a ti, ¿qué tan a salvo puedes estar si las compañías online más grandes en el mundo tienen brechas? No hay defensa contra el robo de información si tu información está en una gran compañía que es infringida. Lo único que puedes hacer es protegerte a ti mismo de futuros daños resultantes de los ataques de relleno de credencial, esto es sentido común y la mejor manera de estar protegido.

Utiliza multi-factor de autenticación. Otra manera de ver esto es un proceso de inicio de sesión de dos o tres pasos, por ejemplo, si el proveedor de servicios ofrece registro de celular con un código de acceso para aumentar tu inicio de sesión, entonces úsalo, todo lo que debes hacer es proveer tu número de teléfono celular y cada vez que vayas a iniciar sesión te llegará un código de acceso a tu celular como mensaje de texto. Simplemente ingresa el código de acceso en el debido espacio de la página web y accede al sitio. Esto impedirá cualquier ataque de relleno de credencial.

El resto de la defensa desafortunadamente miente con el proveedor del sitio web o servicio. Puedes ciertamente escribir al departamento de atención al cliente y solicitar que brinden servicios de seguridad, cosas como bloqueos de cuentas y limitación de tasas estableciendo un límite en el número de veces que puedes intentar ingresar, antes de que cierre la capacidad de iniciar sesión. Esto es una excelente medida contra los ataques de relleno de credencial. Pregunta al proveedor de servicios o al sitio web si hacen monitoreos de credencial, pueden controlar las credenciales comprometidas que circulan en redes oscuras o que son vendidas en mercados negros en línea. Y pregúntale al departamento de servicio al cliente si utilizan Captcha, un simple servicio de selección de fotografías que requiere un usuario consciente y mitiga todos los ataques de relleno de credencial hechos por un sistema de software autónomo. Entre la seguridad del sitio web y la utilización de una única contraseña y nombre de usuario, estás a punto de estar tan protegido como puedes estar.