BILINGUAL ARTICLE - NOTA BILINGUE

Cyber Security for small business: Are your passwords passable? By JM Lucian for ABClatino

In our previous article, we touched on 5 free ways to improve cyber security for businesses. We wanted to expand on each of the 5 areas to provide more information on the why's and how's.

Passwords are our first line of defense when it comes to cyber security. At the most basic level, they protect our personal information and important data by slowing down or defeating attacks from the bad guys.

Often, the first question people ask is, "Why do I need a strong password?"

I used to work for a company where all the executives used Macs. One of the things they loved about their Macbooks was they didn't have to login to begin using it. (For those who don't know, you can set up your Windows PC to do the same thing.) The one good thing that came out of it was when someone left a laptop in a cab, the cab driver was able to access the user's personal information to contact him. In another instance, however, someone left their laptop at a sporting event, and a few weeks later, identify theft ensued.

The point of that anecdote is to illustrate that if your device is protected by a weak password like "Password123" or something similarly common, just about anyone can get into your laptop and access the information on there. As an IT admin, part of my job was to re-issue laptops. When users left the company, many left digital copies of their personal documents on these machines – everything from vacation videos, family pictures, tax returns, scanned copies of social security cards, passports and credit cards, etc.

Keeper Security provides a list of the most commonly used passwords in 2016. If you are using one of these passwords, consider yourself warned. Even amateurs can get into your computer, email, websites, alarm codes, and whatever else you keep on your computer or online.

According to Sophos, "55% of net users use the same password for most, if not all, websites." Best practices recommend having a different password for every account. With roughly 130 accounts registered per email address in the US, can you blame them? One solution, if you have too many passwords to remember, is a password manager. There are many of them available so do some research to see which ones meet your needs. I've used Dashlane, Lastpass and Roboform which have their pro's and cons.

Whether or not you use a password manager, you should always implement the following best practices when creating a password:

- Choose one that has at least 8 characters
- Don't use dictionary words, names or birthdays
- Use a combination of upper and lower case letters, numbers and special characters.
- Don't use sequential characters (9876abcd) or repetitive characters (zzzzZZZZ)
- Don't use the name of the service you are using (google)
- Don't keep passwords on stickies

On March 31, 2017 NIST (National Institute of Standards and Technology) updated their Digital Identity Guidelines with recommendations that favor the user. This places more of the onus on website owners and organizations to keep your information secure, but that doesn't mean you get off scot free. As these updated recommendations were recently released, it will be a while before most organizations implement them. In the future, life as a password creator will get easier, but we still have to do our due diligence in the meantime.

If you have any questions or comments, please reach out to us at info@misits.com

Seguridad cibernética para pequeñas empresas: ¿Son sus contraseñas aceptables? Por JM Lucian para ABClatino

En nuestro artículo anterior, se habló de 5 formas gratuitas para mejorar la seguridad cibernética para las empresas. Queríamos ampliar cada una de las 5 áreas para proporcionar más información sobre el por qué y cómo.

Las contraseñas son nuestra primera línea de defensa cuando se trata de seguridad cibernética. En el nivel más básico, protegen nuestra información personal y los datos importantes mediante la disminución o la derrota de los ataques de los malos.
A menudo, la primera pregunta que la gente hace es: "¿Por qué necesito una contraseña segura?"

Solía trabajar para una empresa donde todos los ejecutivos usaban Macs. Una de las cosas que les encantó de sus Macbooks fue que no tenían que iniciar sesión para comenzar a usarlo. (Para los que no saben, puede configurar su PC con Windows para hacer lo mismo). Lo bueno que salió de ella fue cuando alguien dejó un ordenador portátil en un taxi, el conductor de la cabina fue capaz de acceder a la Información personal del usuario para ponerse en contacto con él. En otro caso, sin embargo, alguien dejó su computadora portátil en un acontecimiento que se divierte, y algunas semanas más adelante, el hurto de la identificación siguió.

El punto de esa anécdota es para ilustrar que, si su dispositivo está protegido por una contraseña débil como "Password123" o algo similarmente común, casi cualquier persona puede entrar en su computadora portátil y acceder a la información allí. Como administrador de TI, parte de mi trabajo era volver a emitir portátiles. Cuando los usuarios abandonaban la empresa, muchos dejaban copias digitales de sus documentos personales en estas máquinas, desde videos de vacaciones, fotos familiares, declaraciones de impuestos, copias escaneadas de tarjetas de seguridad social, pasaportes y tarjetas de crédito, etc.

Keeper Security proporciona una lista de las contraseñas más utilizadas en 2016. Si está utilizando una de estas contraseñas, considérese advertido. Incluso los aficionados pueden entrar en su computadora, correo electrónico, sitios web, códigos de alarma, y cualquier otra cosa que mantenga en su computadora o en línea.

Según Sophos, "el 55% de los usuarios de la red utilizan la misma contraseña para la mayoría de los sitios web, si no todos". Las prácticas recomendadas recomiendan tener una contraseña diferente para cada cuenta. ¿Con aproximadamente 130 cuentas registradas por dirección de correo electrónico en los EE.UU., se puede culpar a ellos? Una solución, si tienes demasiadas contraseñas para recordar, es un administrador de contraseñas. Hay muchos de ellos disponibles así que hacer algunas investigaciones para ver cuáles satisfacer sus necesidades. He utilizado Dashlane, Lastpass y Roboform que tienen sus pros y sus contras.

Si utiliza o no un administrador de contraseñas, siempre debe implementar las siguientes prácticas recomendadas al crear una contraseña:

- Elija uno que tenga al menos 8 caracteres
- No utilice palabras, nombres o cumpleaños del diccionario
- Utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- No utilice caracteres secuenciales (9876abcd) o caracteres repetitivos (zzzzZZZZ)
- No utilice el nombre del servicio que está utilizando (google)
- No mantenga las contraseñas en stickies

El 31 de marzo de 2017 el NIST (Instituto Nacional de Estándares y Tecnología) actualizó sus Directrices de Identidad Digital con recomendaciones que favorecen al usuario. Esto coloca más de la responsabilidad en los propietarios de sitios web y organizaciones para mantener su información segura, pero eso no significa que usted salga libre de scot. Como estas recomendaciones actualizadas se publicaron recientemente, pasará un tiempo antes de que la mayoría de las organizaciones las implementen. En el futuro, la vida como creador de una contraseña será más fácil, pero todavía tenemos que hacer nuestra debida diligencia mientras tanto.

Si tiene alguna pregunta o comentario, comuníquese con nosotros a info@misits.com