Cybersecurity: Protect Your Passwords

Have you ever received an email from a friend saying their email account had been hacked? If you are like most people, you have received several of those emails over the years. Hacking typically occurs when a person's email password has been obtained by an unauthorized party. It's actually quite simple for a hacker to obtain passwords and infiltrate an account.

Type "password cracker" into a Google search and the results will contain dozens of pages of password crackers available for free or at a very low cost. Good password crackers can decipher any password with seven or fewer characters in mere seconds. Now think about how safe (or not) your online banking password is (and other sites with your data).

If your password has fewer than 8 characters, or has a word that is in the dictionary, you are a prime candidate to have your password cracked. Even if you substitute characters, such as a "5 "instead of an "S" or a "3" instead of an "e"—the bad guys know those tricks.

We're not trying to scare you. Our recommendation is to prevent password cracking by having every internet password :
- contain 8 or more characters,
- be totally random,
- contain upper and lower case characters, numbers, and special characters.

Also, every account should have its own unique password so that if a hacker obtains the password for one, they won't have it for any others.

Now you're probably saying to yourself, "Nobody can possibly do that!" If you choose, you can use password management software (two good and free options are lastpass.com or RoboForm Everywhere). Let the software generate strong passwords of 8 characters or more for each account. The software will remember your passwords and safely store them. Password management software l even protects you from keystroke loggers and phishing attempts. The software is free, and is much easier than making up, and remembering, your own passwords.

We want you to know that The Biondo Group considers protecting your personal data a top priority. To ensure that your data stays safe while in our hands, we have a team dedicated to this purpose. Patrice Singleton, Chief Information Security Officer; Jean Pavek, Chief Compliance Officer; and Greg Miller, Chief Information Officer are continually working to ensure that we have the best security practices deployed in our office.