Password Security

Question: What percentage of your daily business is conducted via email? Routine things like ordering from suppliers, receiving customers' orders, confirming orders and shipment updates.

Question: How much has that percentage grown over the past five years? Two years? One year?

Question: When was the last time you upgraded your network firewall appliance, upgraded your antivirus/spam software or changed your email password?

Imagine this scenario: John Doe has a successful small awards business named 'John's Awards & More'. Mr. Doe has four employees in addition to himself. One day, Mr. Doe receives an email from a familiar customer, although the message is somewhat vague, it appears to be an order. Within the email is a link which looks to provide additional information for the possible order. Mr. Doe clicks on the link and immediately realises that this is just another spam email and deletes it from his inbox. End of story? Not quite.

By clicking on the link in the email Mr. Doe inadvertently executed a script to run inconspicuously in the background which exploits a vulnerability in his operating system, which in turn allows a hacker to obtain private information on his computer. Email account username, Facebook account username, bank account username, etc.

This hacker runs another script to 'hack' into Mr. Doe's Facebook account and send out spam messages using another script. This in turn generates more 'leads' for the hacker. In the meantime, the hacker is using variations of the found password to hack into other accounts of Mr. Doe.

The next day Mr. Doe is preparing payroll for his four employees only to find that the John's Awards & More account is showing a negative balance. Mr. Doe is at a loss. He has antivirus software. He has spam blocker software. How did this happen?

According to a report recently released by the risk management company Deloitte: "In 2013 more than 90% of user-generated passwords will be vulnerable to hacking". To put that into perspective, there are 94 characters on the standard keyboard. An eight-character password would be one of over six quadrillion possible combinations. The report goes on to say: "In a study of six million user-generated passwords, the top 10,000 most common passwords would have accessed 98.1% of all accounts." Add to this the fact that the email account holder is more often than not, the last person to know that their account has been hacked.

A study by credit checking firm Experian found that the average computer user has 26 password-protected accounts. Maybe you have more. Maybe less. Ask yourself this question: how many password-protected accounts do you access using the same password? Spoiler alert: the average is five passwords used across that 26 account range.

The online accounts targeted most are Yahoo email (27%), Facebook (23%) Gmail (19%) and Windows Live (15%). Are you hosting your company's email through a free service? What security measures are you implementing? It's one thing to expose your personal email to these vulnerabilities, but can you risk your company's viability to lax security measures?

So now what? Is your business large enough to have a full-time network security specialist? A part-time specialist? Maybe you're using some type of contracted services. That's a great position to be in. Utilise those services and ask questions. Review policies and procedures for password administration on all company related online accounts.

But what about the small business? The 'home' business, the Mom and Pop shops? Some rules to follow are:

1. Change your password. Set up a schedule to change your account passwords monthly. Set a reminder to do so on your calendar or mobile phone. Changing passwords monthly is one of the most effective security measures you can take, but only if you follow through with it.

2. Make sure you have a 'secure' password. Use at least eight characters. Mix in numbers and other special characters. Utilise a capital letter but not necessarily the first letter. A good example would be something like 'gh4Lm#2i'. A mixture of upper and lower case letters, numbers and special characters.

3. Separate personal and business accounts. Do not use your personal email account to do business and vice versa. In a home business, try not to use the same computer for business and personal account access. If your personal account gets hacked and user information is compromised, you want to limit the cross over damage that can occur.

4. Use reputable antivirus/spam software. There are several 'free' options available but remember the saying: 'You get what you pay for'. Some 'free' options may be adequate, but do you want to take that chance? You want to be sure that support is available should you have a problem. Some of the top phishing sites portray themselves as free or inexpensive antivirus/spam alternatives.

With our increasing reliance on digital communications, we all need to be aware of the recommended 'best practices' and implement these into our daily business routines.

Our thanks to Patrick Quittem at JDS Industries, Inc for writing this article. Patrick has more than 20 years of experience in design, marketing and information technology. He can be contacted at patq@jdsindustries.com.

For more information on JDS Industries, Inc. please visit the website at www.jdsindustries.com.