AIM

AIM CYBER

High-touch services to help you navigate modern cyber threats.

EX-EMPLOYEES STILL HAVE ACCESS

It is doubtful that any company executive believes that ex-employees should still have access to systems and applications.

Yet, recent research shows that almost 25% of people who left a company still do have access. Even if only one person uses it, the results can be data theft or sabotage, or both.

How is this possible you ask? This seems so easy to prevent.

A few factors contribute. Password sharing, while often prohibited, still occurs. Over 40% of polled workers admitted to sharing their password, not just with co-workers but with contractors, family members, and friends.

Making matters worse is that the employees most likely to share their password are management, who have access to more systems and data, including the most sensitive personal and company information.

The reasons given for password sharing revolve around convenience. People don’t want to do anything that will reduce their productivity or delay any thing they are working on. Needing to change passwords and then remember a new one, or the use of two-factor authentication are viewed as delaying.

Employees often use the same password on all systems including personal ones. This increases the chances of a password being compromised. While contrary to all advice on password security, they do this because they can remember the one password. But of course, if the password is stolen, shared or otherwise compromised, it will provide access to as many systems as the user can access. Password stuffing, a common technique used by cybercriminals where they try a stolen password on many sites will deliver a treasure trove of information if the same password is used on multiple systems.

One other risk is failing to disable a user’s access immediately upon the person leaving the firm, voluntarily or not. Disabling all access needs to be done immediately. Waiting even one day is a risk.

Remember to disable all access, every system and application the user had access to. If the person was considered an unhappy or disgruntled employee, a complete scan should be done on all systems they accessed in case they uploaded malware before leaving.

Protecting information entrusted to you is essential to the continuation of your business. Creating and enforcing password policies and procedures is an essential part of this. Without enforcement the policies and procedures are worthless. People will read them, say they agree, and do what they want. The penalties must be strong enough to make people comply.

Remember, passwords are the keys to your business house. Protect them as you do the keys to your physical office and printed confidential information.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.