CYBER SECURITY AND YOU

If there's one theme from 2016 that will ring through into 2017, it's online security and securing your data.

For businesses, the cost of a breach can be devastating and time consuming. Placing proper cyber security protocols in place can help reduce the likelihood of data breaches and make recovering from a security event much easier, should one occur. Here are seven tips to help get your business' cyber security ready for 2017.

1. Establish security training for all employees

One of an organization's weakest security points is the employee and how they utilize technology such as email and online access. Developing protocols for protecting your business's data so that everyone can be on the same page for cyber security is the first step in getting everyone on the same page. Establish cyber security training for all new and existing employees. Because knowledge can fade over time, and protocols can change, offering periodic review trainings should also be a priority.

2. Encryption and Enterprise Protocols

Encryption has been used since ancient times to code messages that could only be read by authorized parties. Today, encryption technology uses advanced algorithms to make data unreadable except by those with the correct key. Encryption is a must for businesses protecting sensitive information, such as customer credit card information or government issued data.

3. Keep software and browsers up to date

Vulnerabilities often occur when software and browsers are not updated on a regular basis. Software manufacturers periodically release updates for their programs, which often include security updates. Take advantage of these updates, and don't leave your operating systems, browsers, and anti-virus software vulnerable.

4. Use multi-factor authentication technology

When two factor authentication is applied to an online account or system, there is an instant benefit of extra protection. This way, even if your password is not as strong as it should be or the account is compromised, there is still another line of defense. Two factor authentication (TFA) is a two-step process of identifying an entity at a point of access into the system. This type of protection is available usually with a secure token or cell phone device. Services such as Gmail offer this option as a way to secure your account.

5. Ensure the security of Wi-Fi networks

Access to your business's Wi-Fi network is a huge benefit to cyber criminals. Keeping your network safe requires a few extra steps than setting up a home router. Use a firewall, and hide your network name from broadcasting to help protect it. Require a strong password for Wi-Fi access. Check out the Department of Homeland Security's Cybersecurity Framework website for additional tips on this subject.

6. Create a culture of "personal responsibility"

The trick to encouraging people to care about cybersecurity is by creating a sense of ownership. Creating this culture of responsibility to protect sensitive information, allows an organization to focus on larger threats knowing that everyone in the organization is vigilante to external and internal threats. There are many forms of insider threats which can be safeguarded against by implementing a solid culture of confidentiality and responsibility.

7. Use Bank Products such as Check and ACH Positive Pay

Positive Pay is a service provided by banks that has proven to be an effective weapon against check and ACH fraud. If you are a victim of a security breach Positive Pay can protect your bank account against unauthorized payments and transactions. There are several versions of Positive Pay so for more details and questions contact Oxford Bank's Treasury Management department for more information at 248-814-6506.