PROTECT YOUR ASSETS:

TOP 5 SMALL BUSINESS CYBERSECURITY TIPS

by Jamie Saker

Think about all of the data on your business computer or on the cloud. Would your small business survive if a hacker were to steal those assets or lock down your data for an extended period of time? This is what you are risking if you're not focusing on small business cybersecurity.

There are a number of things you can do to protect your company from cyberattacks and prevent a small business data breach.

#1 | START WITH A PRAGMATIC RISK ASSESSMENT.

Identify any assets that are at risk of a cyberattack and whether your business would survive if they were stolen or locked by a hacker for an extended period of time. Look at anything saved locally on your computer, anything saved on your servers and anything cloud, or web based. This includes your bank accounts with electronic access, customer data and records stored on your business computer, and even your business scheduling software.

For example, If a business has a truck delivery schedule laid out for the next 90 days and it's locked or wiped out by hackers, all the revenue from the work could be gone. Many small businesses don't have the resiliency to have a quarter of their year wiped out.

#2 | CHOOSE GREAT PARTNERS FOR YOUR SMALL BUSINESS CYBERSECURITY NEEDS.

Many small business owners don't have the staff or resources to manage the intricacies of small business cybersecurity. This is where your partners come into play.

Your partners include your product suppliers, software suppliers, your computer supplier and your business's bank. Choose suppliers, vendors and partners who are passionate and proactive about small business cybersecurity and who are committed to keeping your information, your customers' information and your finances protected from hackers. You can eliminate a lot of threats simply by not bringing in products and services from companies with weak cyber- security practices.

#3 | USE PASSWORD MANAGERS AND TWO-FACTOR AUTHENTICATION.

For maximum security, use a unique password on all of your accounts as opposed to using the same, or a similar password for everything. This significantly reduces the likelihood of multiple accounts being compromised after a hacker discovers a single password.

With so many unique passwords to remember, you will want to use a password manager to help you keep track of everything. Password managers, like LastPass, Keeper or Dashlane will manage all of your passwords under a single master password.

Two-factor authentication, like the kind provided by authenticator apps such as Duo, LastPass or Google Authenticator will require the user to enter their password, but then also ask for a second confirmation, many times in the form of a push notification on a mobile device, or a biometric like a fingerprint or a facial scan.

#4 | TEST YOUR SMALL BUSINESS CYBERSECURITY; SIMULATE A HACK ON YOUR OWN SYSTEM.

Some businesses will run scenarios with their team where they try to breach their own systems to help identify any holes in their cybersecurity efforts. Try running an exercise with two teams, one trying to hack your business and the other trying to defend it.

#5 | ESTABLISH A TWITTER ACCOUNT TO MONITOR CYBER THREAT INTELLIGENCE FEEDS.

Establishing and monitoring a Twitter account for the dedicated purpose of monitoring cyber threat intelligence feeds is a low cost yet highly effective way to monitor cyber risk. The following accounts are ones I recommend following to get a solid open source intelligence footing for your organization's security program:

Organizations
@Cyber - CISAgov Cyber News
@TheHackerNews - Independent Cyber News
@BleepingComputer - Independent Technology & Cyber News
@Threatpost - Fast Breaking Security News
@TheCyberWire - Cybersecurity News Daily Podcast

For more information on Small Business Cybersecurity check out our Biz Buzz Blog Articles:
Improve Small Business Cybersecurity | Business Email Compromise