Beat: Business

Entrepreneurs Are The New Victims Of Cyber Criminals

Starting up your business, read this!

Washington, D.C , 02.12.2018, 19:31 Time

USPA NEWS - Cybercrime´s have reached a new peak during the past decade. It is assumed that large businesses and corporations are more prone to these threats, since huge amount of cash and resources are involved. However, not everyone knows that entrepreneurs and small businesses are more vulnerable to cybercrime. As per the Internet Security Threat report of 2017, it´s estimated that 43% of cybercrime target small businesses.

Cybercrime´s have increased mainly due to the careless behavior of entrepreneurs. They take risks without even knowing about the consequences of their actions. Business owners should be more aware of the activities that may destroy their business.

A majority of businesses use social media sites to spread awareness about their brand, attract more customers, and retain their customers by interacting with them. It´s a common practice to share personal information on public accounts.

However, cyber criminals may use this information for identity theft. With the help of your full name and date of birth, they can obtain social security number of your business.Around 1,209 breaches were reported in 2016, which resulted in the exposure of 1.1 billion identities.

Oftentimes, entrepreneurs need to travel for business purpose. Business owners may connect to public Wi-Fi of airport and hotel to work online. Moreover, many people allow their systems to automatically connect to an open Wi-Fi, whenever service is available. However, it leaves your business information vulnerable to cyberattacks.

Your computer or mobile phone may contain crucial business information. Many cyber criminals create shadow networks that are similar to public Wi-Fi networks, but spy on user activities. If your system connects to such a network, they can extract confidential information and make profit with this business information.

Most people use passwords that are easy to guess. It makes their online accounts more vulnerable to hacking attacks. Hackers may use different tools to crack password and get access to online bank accounts or cloud data storage systems.

Phishing attacks have also become quite common these days. Every 1 in 131 emails contains malware. Employees of small businesses often receive phishing emails. If they click on the attached links, malware software are installed on the system. It transfers the control of the system to hackers. They can look into confidential information and may interfere with business activities.

Ransomware is the relatively new form of cyberattacks. Cyber criminals take control of business system by installing malware. They cease business operations and ask for a hefty sum to unlock data. They threaten business owners to delete the entire information or misuse it if their demands are not accepted. Around 463,000 ransomware cases were reported in 2016.

Smartphones make our lives easier. Wi-Fi, camera and GPS systems in a single device allow users to perform various tasks in a convenient manner. Modern smartphones have large memory capacity, due to which users can store a lot of information. Entrepreneurs use these features to monitor business activities on the go.However, hackers may access this information by installing malware on their devices.

A majority of businesses store business information in cloud services. It saves space and simplifies the tasks of accessing and managing bulk data. However, despite its several benefits, cloud storage also poses certain risks for businesses. The major concern is data security. It´s relatively easier for hackers to break into cloud storage. Once they get their hands on confidential information, they may take control of business operations.

Cyber criminals attack business systems in search of valuable data. They look for employee information and details of financial resources of the company. With the help of credit card number, social security number, email address, residential address, birth dates and bank account information, they can create fake accounts for fraudulent activities.

Most small businesses are not aware of the importance of security measures. However, preventive measures are must if you want to keep cyber criminals at bay. Invest in online security before any intruder takes control of your information systems and harms your business.

It is essential to install anti-malware software and firewall on information systems.These security solutions keep an eye on online activities and eliminate threats in a timely manner.Update the software regularly, so that they can deal with latest viruses,Trojans, spyware and ransomware. While browsing internet, the online security tools alert you of any suspicious activity and protect your system and network from infected files.

Train employees on security threats and their impacts on the business. Due to the lack of knowledge, they are more likely to fall in the trap of cyber criminals. Also, strict password policies should be enforced. Always use strong passwords for accounts, so as to increase protection. Employees can install secure password management systems. These apps allow them to save all their passwords in a single space. They can also generate strong passwords using random combinations.

Install latest versions of browsers and other software. They are more capable of preventing cyberattacks and provide efficient security for your business. Use secure network protocol to transfer confidential information. It is the most effective way to protect information from hackers. Moreover, data files stored in system memory should be encrypted to prevent unauthorized access.

Small businesses ought to take protective measures to reduce the risk of cyberattacks. More than 60% of small businesses have to shut down their operations within 6 months of a cyberattack. They are more vulnerable than ever to cyberattacks. Criminals use modern tools and techniques to get hold of confidential information. It´s about time that entrepreneurs should take drastic steps to improve cyber security.

Article online:
https://www.uspa24.com/bericht-14579/entrepreneurs-are-the-new-victims-of-cyber-criminals.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Dr. Raida Al-Awamleh

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile

info@unitedpressassociation.org
info@gna24.com
www.gna24.com