Online Business Security

PURDUE EXTENSION | COMMUNITY DEVELOPMENT
DIGITAL READY
Expanding Your Community's Online Presence

DISCLAIMER: This online business security handout is not intended to be comprehensive. Rather, it is for informational purposes only. This handout is an adaptation from the Security Squad Workbook published by the Southern Rural Development Center & University of Nebraska-Lincoln.

Equipment & Software Inventory – tallying what you have

Consider keeping a list of your business equipment and software licenses. This information will come in handy when dealing with insurance. Regularly (every 6 months) update the equipment and software inventory. Make sure to include date purchased, purchase price, serial number, MAC address, location in your business or in equipment (in case it is software) and primary users. Keep a hard and digital copy of inventory at your home or other non-business location.

Passwords – creating strong passwords

Identification and authentication procedures require passwords and are your first line of defense against hacking. Passwords need to be setup for every employee who logs onto any business computer or network. Passwords need to be changed frequently (every 6 months) and contain at least eight characters including numbers, text and special characters. If you think any password has been compromised, change it immediately. Add password-activated screen savers to all devices in your business as well and make sure they lock out users after numerous failed attempts. DO NOT use the same password for different accounts!

Backups – making secured copies

Secure backup is very important! Just like paper copies and file cabinets, digital information needs to be backed up. Backup of digital information needs to happen daily to be on the safe side. Both Mac and Windows operating systems have backup options. You can also consider backing up to a third-party cloud provider. It is best to, if possible, have multiple copies of your backups in different locations. For example: flash drives, CDs, and/or magnetic tapes in the office and at home as well as cloud-based accounts would be ideal. Betting on one single backup copy is as risky as not backing up at all.

Online Business Security

PURDUE EXTENSION | COMMUNITY DEVELOPMENT
DIGITAL READY
Expanding Your Community's Online Presence

Viruses – protecting your office from malware

Passwords and other business information can be stolen or deleted by malicious subjects installing malware (or viruses) on your devices or servers. In other words, malware can access your business computers and network through websites, downloads and email. For this reason, it is critical that employees are aware of these risks and under no circumstance open links or download attachments from suspicious emails. Hackers may be able to obtain names and events related to your business and tailor their phishing emails to look more legitimate. Avoid browsing websites that promise cheap deals and/or free things. Install and update frequently antivirus software on each business device and make sure other business software, including Windows, updates frequently. These safe practices are very important, not only to safeguard your business data, but also if your business sells online, it safeguards your customer's data.

Wireless – limiting your exposure

If your business offers wireless to its customers, make sure it is a different network (public) than the one used for your business computers and activities (private). For the public network, use wireless user agreements where a person who uses that connection agrees to use it for lawful purposes. In addition, ensure the private and public networks are secure (require password to log onto network). Otherwise, anyone within range of your wireless signal can connect to the network. When away from the office avoid, when feasible, logging into an open (unsecure) network to conduct business related activities. For example, logging to your business server and/or checking your business email. Doing this may expose your business login credentials to malicious parties.

Firewalls – stopping hackers at the door

Another line of defense against hackers is a firewall. A firewall is a software or hardware that filters incoming internet traffic into your business network and devices. Hackers like to launch random attacks on the Internet to see which are vulnerable. Firewalls can detect this activity and block it. Hardware firewalls are installed between the Internet and your business network and can be managed using a web-based interface to configure its access rules. Software firewalls are installed on each business device and allows users to control access.

Online Business Security

PURDUE EXTENSION | COMMUNITY DEVELOPMENT
DIGITAL READY
Expanding Your Community's Online Presence

E-commerce – buying and selling safely online

Trust, or lack of, has a huge impact on online sales. If you do not trust a retailer, you more than likely will not buy online from them. There are safety protocols that will help your customer trust you. If your business collects and transmits customer data it should secure transmissions using a Secure Socket Layer (SSL) encryption protocol. The server on which your business relies for online transactions needs to have a SSL certificate. A customer can know if their connection to your business website is secure by looking for a locked padlock on the browser status or a green safety bar in the address bar. In addition, the URL will add an "s" to the "http" portion ("https"). To ensure the customer is visiting the business website and not impostor websites, the business website needs to be authenticated by a digital authority. Make sure a privacy policy is shown to customers letting them know how your business will and will not use their information and your contact information is easy to access in case they have any questions. The Fair and Accurate Consumer Transaction Act of 2003 requires any business to properly protect and dispose personal information of their customers and employees. Some measures you can take to comply with this is to limit employee exposure to credit card information, do not send email or written correspondence that include a customer's full credit card number, and others.

Employee policies – protecting the company and employees

Any business, regardless of size, should develop an acceptable use policy (AUP) that outlines the acceptable use of business devices, software and customer data as well as consequences for not following the AUP. This AUP could include a privacy policy clearly outlining that all business related information, including customer data, is confidential. Policies should also include smartphone use and working from home considerations.

PURDUE EXTENSION | COMMUNITY DEVELOPMENT
DIGITAL READY
Expanding Your Community's Online Presence

Find your next workshop!
Scan the QR code or visit:
cdext.purdue.edu/dr

1-888-EXT-INFO • www.the-education-store.com