## Covid-19 Best Fraud Prevention and Cybersecurity Practices for your business.

### I. Increase security for online meetings

As social interaction increasingly shifts to Zoom and other video conferencing platforms, "Zoom bombing " has become a much-discussed form of disruption. In an effort to curtail uninvited participants, these platforms have implemented measures such as requiring passwords upon joining meetings. Users can take added steps to further ensure the integrity of their online meetings by designating co-hosts or moderators to monitor the chat room and step in, if necessary. Users can also take advantage of enhanced privacy features like a virtual "waiting room" that lets hosts see who is attempting to join prior to allowing access. Also, users are encouraged to generate random meeting links for extra privacy.

### II. Take cybersecurity measures when working remotely

Experts recommend using a strong password for home Wi-Fi, avoiding public and unprotected networks, and using a virtual private network (VPN), which is a service that shields internet users by encrypting their data traffic. Use secure wireless connections for printers and wireless network expanders. Use only reputable mobile device scanning apps and avoid "easy" solutions, such as forwarding business documents to personal email accounts.

### III. Exercise responsible management of hard copy documents

Employees may be printing more documents at home or using files and documents that are normally kept in an office. Communicate to employees the proper way to dispose of confidential documents, such as not throwing them in the household trash, for example. In addition, employees should use care if they are sharing a workspace with roommates or others who may inadvertently be exposed to confidential information..

## #TechTips for business owners

Any device that connects to the internet is vulnerable to risks. The best defense is to keep device security software, web browser and operating systems up to date. Be Cyber savvy by turning on auto-updates.

No matter how long and strong your passphrase is, a breach is always possible. Make it harder for cybercriminals to access your account by enabling multi-factor authentication.

## Contact Us

**Haverhillbank.com**

**(978) 374-0161**

**Visit your local branch**