# HFTP 2019 Club Forum

October 26, 2019 • Rosen Centre Hotel • Orlando, Fla.

## Question: Important IT Security Measures

The following list was compiled by the 28 plus attendees to the HFTP 2019 Club Forum. The task assigned to the groups was to list important IT safety measures to prevent hacking and other cybercriminal activity. The below is a compilation of all the suggestions.

- Password maintenance – strong passwords and frequent updates/changes; protect how passwords are kept
- Network structure – maintain firewall and VPN
- Two factor authentication/tokenization
- Software monitoring
- Remote access – securely set up; use VPN
- Download restrictions
    - Turn off saving to c-drive
    - Prevent use of thumb drives (or have them scanned)
    - Have a process for downloads
- Ongoing training for employees on security measures and current cyberattack methods
- Auto logout
- Segregate Wi-Fi: Guest network and club admin network (hide from public view)
- For guest Wi-Fi; have the guest use time-out
- Acknowledge use of unsecure Wi-Fi; password protect wireless access
- Block domains by country
- Email filtering; have incoming emails scanned
- Keep anti-virus software updated
- Operating system patches – clear by IT dept
- Test your back up system
- Make sure back up system is secure
- Malware protection software
- Do not publish email addresses on website
- Do not share passwords
- Upon the dismissal of an employee, remove access immediately (change passwords, etc.)
- Train security cameras on IT equipment
- Monitor mobile device access
- Monitor access of third parties to your system
- Only give access to systems where necessary
- Verify wire transfers by phone

- Check IDs of outside service providers who are gaining access to your system/network
- Separate servers (can be done virtually)
- Have it set up to get a warning if an intrusion is detected
- Conduct penetration tests
- Lock down POS so that it is not connected to the Internet
- Dedicated IT resource (whether onsite or outsourced)
- Schedule vendor maintenance – and make sure that the person who comes in is the person scheduled to do the maintenance
- Monetary processing: EMV readers for cards and PCI compliance
- Use encryption for sensitive information sent by email