Best practices to HALT HACKERS looking to exploit the pandemic

Compliance Officers: Stay ahead of cyber thieves using COVID-19 to mask an IT intrusion. Here's what you can do...

Revisit telecommuting policies and procedures, with an eye toward addressing risks related to remote access. Communicate the basics, such as:

- Encryption requirements
- Prohibitions on sharing work devices and passwords
- Permissible activity on personal devices
- Public wi-fi as off limits
- How to report lost or stolen devices immediately
- Two-factor or multi-factor authentication

Don't assume IT has everything covered. Drill down for specifics about:

- The latest antivirus software update; get assurance the newest versions are downloaded and implemented
- Emerging cyber theft tactics and ways to preempt them;
- Defenses currently in place and potential vulnerabilities:
  - » Is your firewall or sonic wall effectively blocking unwanted emails and warding off malicious activity on your organization's server?
  - » Do you utilize any anomaly-detection software?
  - » Are you actively and regularly auditing and monitoring staff usage of all electronic platforms where patient information resides?
  - » Are you enforcing two-factor or multi-factor authentication?
  - » Is your spam filter active, up-to-date, and effective?