CYBERSECURITY BEST PRACTICES FOR THE HOLIDAY SEASON

GILL TECH
COMPUTER SERVICES

'Tis the season to be jolly. But 'tis also a season to feel pulled in many directions. For many organizations, this is a peak season. For others, things slow down, and people are able to take a long-awaited vacation.

Wherever you fall on the stress spectrum, these best practices can boost your holiday cybersecurity.

Get a Virtual Flu Shot

This is the time of year a lot of people get a flu shot to fend off any outbreaks of illness. Do the same with your information systems. Make sure all your antivirus software is up to date.

Your IT team may have a long to-do list to get through before they take a break, but updates can't wait until they return. Install all security patches and upgrades before closing your doors for days.

Be Ready to Scale

Are your employees like Santa's elves ramping up for the major push before the New Year? If so, make sure your website or internal IT infrastructure is ready to handle the increased load. Don't risk your provider disconnecting you if you get an influx of customers!

Cloud computing may be a good option for you, as you pay for the services you use, as you go. You don't have to invest heavily in new technology, and you're not paying off more IT tools than you need.

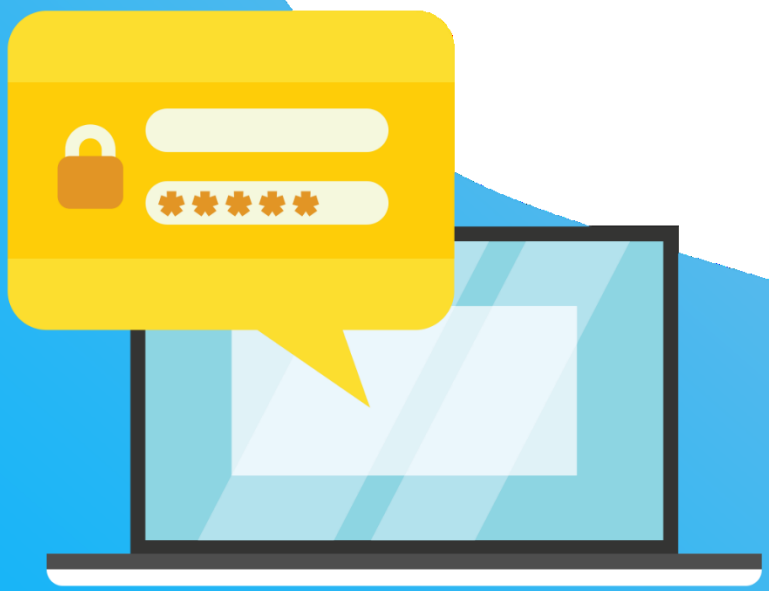
Your cloud provider is responsible for the infrastructure in the cloud. This lets you easily scale up if busy or down if not. Cloud solutions are often a good option for internal systems such as point of sale (POS), as well. With a cloud POS system, you gain the flexibility of working on a desktop, laptop, iPad, or other mobile device.

If you're sticking with an on-premises POS system, ensure that your on-site server is up to the task; you don't want to risk losing any sales this season.

Plan for Change

The end of the year is a prime time for people to move on to new positions or retire. Have a policy in place to revoke access for any employees leaving your organization. The individual's password should no longer work after their last day of work.

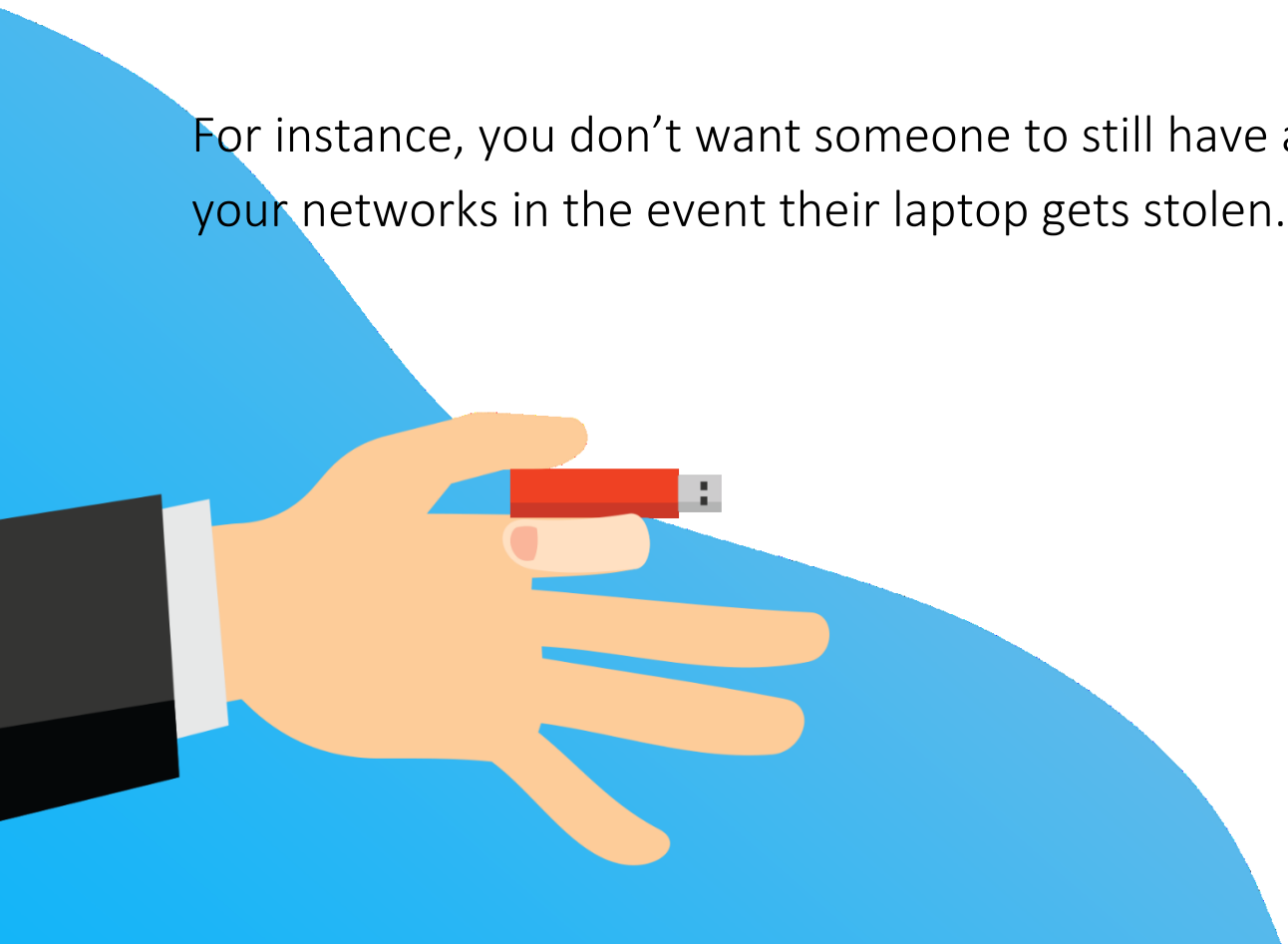
Also, keep an eye on employee access to your company's information system. Disable all network and system access rights for exiting employees.



Reclaim any business devices you provided. Use remote mobile monitoring to wipe any personal devices they used for work. In an exit interview, ask about any thumb drives or ID access cards employees may have.

Your former employee may be leaving on good terms and have no malicious intent. However, don't risk them inadvertently exposing you to cyber risks.

For instance, you don't want someone to still have access to your networks in the event their laptop gets stolen.



Make Holiday Travel Safer

Don’t take the “season of giving” mantra too literally. If traveling this month, don't give cybercriminals access to devices and data. This means being wary of public Wi-Fi networks. Your data is not protected on unsecured networks.

So-called “juice jacking” has also grabbed the headlines recently. Bad actors steal information from, or install malware on, phones plugged into public USB charging stations. The practice is not as common as the fear-mongering headlines will have you think, but it still makes sense to travel with your own phone cord and portable charger.

Plan for Remote Access

Some businesses run through the holidays, whereas others shut down completely. Or maybe you'll try a hybrid of the two. It's still likely that some of your employees are going to need remote access to your business data. Payroll, for instance, doesn't get to skip writing checks because the office is closed.

Set up a remote-access virtual private network (VPN) to establish secure remote connections. This lets users access network resources as if on-site without risking your cybersecurity. At the same time, IT employees avoid the repetitive tasks that threaten to take up the workday. Skilled tech workers can tackle challenging tasks while an MSP handles the routine.

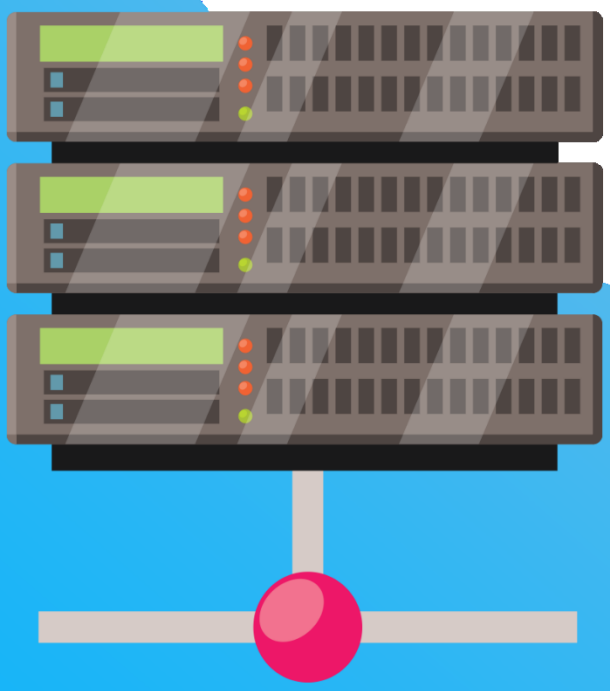
Think About Your Backups

Remember Y2K? Businesses worldwide worried about what might happen to their technology as the clocks ticked over to 2000. There's no widely publicized threat like that to worry about this year.

Nevertheless, if your business takes a break, it's a good idea to ensure your backups are off-site while you're away. Otherwise, if something happens on-site in your absence, you could face a tough start to the new year.

We recommend the 3-2-1 backup rule. To be safe, have three copies of your data. Store two on different storage media locally; the third is always off-site.

For the holidays, have another of those other storage media with you off-site. Plus, have a plan in place for how you will access any backup data in an emergency.



Finding the Fa-la-la This Season

Cybercriminals don't take a holiday. Take the proper precautions to protect your information technology and data. A professional IT support team can keep your cybersecurity up to date year-round.

Don't get Grinch grouchy trying to ensure your data and systems are safe. We can help your organization find the fa-la-la light-heartedness of this season. Call us today at (214) 817-8060 for a free cybersecurity assessment.

Gill Tech Computer Services

1001 E. Main Street, Suite A
Midlothian, Texas 76065

Phone: **(214) 817-8060**
Email: **info@gilltechsvcs.net**
Web: **www.gilltechsvcs.net**
Facebook: **facebook.com/MidlothianComputerRepair**