Best Practices for Security in the Workplace

Beware of Phishing Attacks:

- Was the email in question expected?
- Check for inconsistencies in email address, links (hovering is good), domain names.
- Check the body of the email for these things:
  - Unfamiliar greeting or salutation.
  - Bad grammar, spelling mistakes, and ‘voice’ is suspicious.
  - Demands urgent action ('do this immediately').
  - No opportunity to verify ('in a meeting', 'on a call', 'boarding plane').
  - Requests photos of requested purchase (if gift cards requested).
- Check the link of an attachment before clicking on it. (Again, hovering is good).

Social Media Manners

- Keep in mind, information shared on social media is very near permanent - it always exists.
- Review & modify security settings regularly in apps and social media platforms, especially after they make updates.
- Don’t share vital information like birth dates, high school, hometown, current & past addresses, mother's maiden name.
- Too late for #3 you say - then don’t use those items as answers to security questions.
- Be conscience of what you are sharing in the little ‘games’ you see there (That is data mining at its easiest).
- Check friend requests BEFORE you accept them. The actual request may not come from your friend but rather an imposter.
- Even though tempting, avoid using public Wi-Fi spots. These are fertile grounds for hackers.

Best Practices for Security in the Workplace

Security Awareness

- Keep your devices up to date with the latest security patch (Computers, tablets, phones, gaming devices if used to access the Internet).
- Keep all software and apps updated – especially your browsers (Edge, Firefox, Chrome, Safari).
- Install anti-virus/spam filtering software and KEEP it up to date - Anti-virus software companies regularly update their protection against any new virus signatures out there.
- Install a Firewall if possible – “the best defense against attacks is to not let them in”.
- Setup auto-backups or schedule manual backups on a regular basis and store off-site if possible – can be as easy as copying a folder/file to a thumb drive and taking it home with you.
- Beware of popups or any ads that appear on the sides of websites you may visit. Not all are bad but how do you know which one is good or bad.
- Never click links or attachments received without request or without prior knowledge of their coming – definitely if from an unknown user.
- Maintain on-going security awareness training. Pick a day and schedule time devoted to reading some type of security update – be it a newsletter or a website – do it.
- Limit what you install – particularly on mobile devices.
- Use PASSWORDS – contrary to popular belief, “password” or even “password123” are NOT legitimate protection for the security conscience user in ANY program; two factor authentication is even better.

Best Practices for Security in the Workplace

Parental Control software

Make sure any parental control software works with Windows, Mac, iPhone, Android, and Kindle Fire. Covenant Eyes is purported to be one that does and is very popular. There are some free controls out there, such as Bitwarden, that are said to work equally as well. I haven't investigated either of them enough to recommend them. If your children are heavy users of internet, tablets, gaming devices, etc. they are worth the investment. Here are some things to think about:

Exceptional Christian parental control software should include the following features:

- **Real time online activity monitoring–** Using a Christian internet filter with real time content control features allows you to block access to sites immediately in real time.
- **Time control features** – This allows you to set a time schedule or to set limits on each device or per user for how much internet time is allowed each day. This feature helps parents and guardians to ensure internet and online gaming time is limited, providing them time to undertake their homework, studies and other recreational activities.
- **Device tracking**– this feature allows you to track your child's devices on a map using the location tracking feature, some software even gives the ability to add a panic button to your child's smartphone that sends you location-based alerts when there's trouble.
- **Advanced Facebook Monitoring tools**–Allowing you to view status updates, pictures, friends and more on social networks.
- **Call tracking and blocking**– that let you see who your child calls most and be able to block unwanted numbers.
- **Text tracking and blocking** – See who your child texts most, read text messages and set a list of blocked contacts.

Most important 5 things you need to know when selecting the best Christian internet blocking software:

1. A typical family owns between 8 to 20 devices inclusive of smartphones, tablets, laptops and smart TVs. As some children may have access to all of these, it is best to select software that can protect multiple devices.
2. Select software that is compatible with the most popular operating systems such as Windows, Android, iOS, Mac, and Kindle. If your child is using an Android phone but using windows on a laptop, this will ensure both devices can be protected and synced without the need to install different software for each device.
3. Get software with extended reporting of device usage history. This allows you both more time to review and gives you more information to review all at once.
4. Select a user-friendly Christian Internet filter with apps that can be easily installed on the parent's smartphones or that give easy access to a web-based family portal dashboard. Providing the ability to monitor activities and track time usage quickly in real, providing up-to-date information at a click of a button.
5. Get Christian parental control software that offers premium level features (as listed above) to ensure you are equipped with the best information to protect your family.