EmPower HR Cybersecurity Checklist

You Are The First Line Of Defense

You can be the first line of defense when it comes to protecting your company from security breaches. Help ensure that your data, both personal and professional, stays safe by following these cybersecurity best practices.

Managing Your Devices

- [ ] Use password protection on every device that you use–including mobile devices–so that any sensitive or confidential information stored on it will not be easily accessible.
- [ ] Disable auto username and password completion to reduce the likelihood of sensitive or confidential information being accessed by someone who finds or steals an unprotected device.
- [ ] Always install security updates as soon as they are available.
- [ ] Be sure you can remotely wipe your data from your device if it is lost or stolen.
- [ ] Be VERY careful when using public Wi-Fi networks because these networks are highly insecure and can be easily hacked.
- [ ] Use a hotspot on a trusted phone, or when using a public Wi-Fi network, use an encrypted VPN (virtual private network) if possible.
- [ ] Disable file sync and share tools, such as Dropbox, to reduce the likelihood of a data breach.
- [ ] Be careful when entering sensitive or confidential information and do so only on websites that are encrypted (i.e., the URLs begin with “https” and contain an icon of a lock in the URL bar).
- [ ] Use only “safe” stores with robust security controls, such as the Apple Store or Google Play, when downloading apps.
- [ ] Ask your IT department about access to segmentation technologies that can separate your personal and corporate data on the same device so that the corporate “side” of the device can be wiped by IT if the device is lost or stolen (or if you leave the company), while not affecting your personal information.
- [ ] Never use USB flash drives from unknown sources as they are a common source of infection.
- [ ] Perform regular backups of all computer systems, as it allows recovery from a virus, malware or ransomware infection.

Password Authentication Protection

- [ ] Use strong passwords when accessing a corporate system. Typically, the longer the password and the greater the variety of characters it contains (upper case, lower case, numbers, punctuation, etc.), the stronger and more difficult it will be to hack.
- [ ] Change your passwords frequently even without being prompted.
- [ ] Use a unique password for every system because using the same password across multiple systems increases the opportunity for a cyber criminal to hack one password and thereby gain access to multiple systems. Intentionally use fictitious information for security questions to reduce the likelihood of a cyber criminal being able to respond to security questions correctly.
- [ ] Employ authentication appropriate to the sensitivity of the information. (In most cases, IT will establish the level of authentication required for you to access a system, but you often have some control, particularly for personally managed cloud applications and the like).
- [ ] Use a password manager if your company has not implemented single sign-on capabilities, so that you can create very strong passwords without being required to remember them.

Emails, Web Pages, Social Media

- [ ] Be skeptical of any email, web page or social media post that appears to be even remotely suspicious, makes an offer that is too good to be true, or contains strange information.
- [ ] Emails are the most common method for distributing phishing attacks. To protect yourself, ask questions such as:
    - [ ] Do you recognize the sender's email address?
    - [ ] Do you recognize anyone else copied on the email?
    - [ ] Are others in the email seemingly from a random group of people? Do these recipients' last bnames all begin with the same letter?
    - [ ] Is the domain in the email address spelled correctly or is it simply close to the actual URL (e.g., bankofamerica.com vs. bankofarnerica.com).
    - [ ] Would you normally receive an email from this individual?
    - [ ] Does the subject line make sense?
    - [ ] Is the email a response to an email you never sent (e.g., does it begin with "re:")?
    - [ ] Does the URL in the email (if there is one) match the URL in the tag when you hover over the link with your mouse cursor?
    - [ ] Does the email contain an attachment that does not make sense in the context of the email or sender?
    - [ ] Does the attachment end in ".exe", ".zip" or some other possibly dangerous attachment type?

- [ ] Did you receive an email at an unusual time, such as 3 a.m. on a Sunday morning?
- [ ] Is the sender asking you to keep the contents of this email or any requests within it a secret?
- [ ] Does the email contain spelling or grammatical errors?
- [ ] Is there even a hint of extortion in the email, such as a request to look at compromising or embarrassing photos of you or someone else?

- [ ] Be very careful when reviewing your quarantined messages. If an email that seems to be valid has been captured by a spam quarantine, don't assume it was mistakenly identified as spam and don't bring the email out of quarantine without a careful inspection.
- [ ] DO NOT CLICK on a link in an email or open an attachment until you are absolutely certain that the link or attachment is valid.
- [ ] Don't overshare via social media and limit who can see posts or access contact information on your social media properties.
- [ ] Turn off location services that will automatically post your location on social media sites.
- [ ] Turn on out-of-band authentication that will require entry of a code delivered to a mobile device when logging in from a new browser to reduce the likelihood that cyber criminals will be able to access your social media account.
- [ ] Be careful when clicking, liking or sharing as it could inadvertently distribute malware or spam messages to others in your social media circle.

How EmPower HR Can Help

EmPower HR offers a variety of human resource services tailored to your business needs. Let us handle the HR administrative tasks so you can focus on your business and employees.

Learn more at empowerhr.com

EmPower HR