ManageEngine

Cybersecurity Awareness Month

# Cybersecurity Infographic

As the digital space gets irrevocably entangled with our physical world, it's important now more than ever to safeguard our personal data from prying eyes. It's a good idea to periodically review the security practices we follow. We've identified some of the most common areas that hackers tend to target. Let's take a look at some of the dos and don'ts we should keep in mind to keep ourselves safe in the online world.

## Digital Personality

| Dos: | Don'ts: |
|---|---|
| • Use privacy settings to control who can view content you put up online.<br>• Consider how information you put up online may be used against you.<br>• Periodically review your security and privacy settings on all social media channels.<br>• Always verify friend/connection requests.<br>• Check the level of access third-party services (such as games, quizzes, etc.) have via your social media accounts. | • Don't share sensitive work information on social media.<br>• Don't reveal any personal information on anonymous websites.<br>• Don't broadcast your whereabouts.<br>• Don't upload anything you wouldn't want everyone to see. Always assume that anything you put up will be revealed to the internet at large at some point or the other. |

## Applications and Devices

| Dos: | Don'ts: |
|---|---|
| • Keep a track of all your software license statuses.<br>• Keep all software and applications updated to the latest version.<br>• Have a provision to remote lock or wipe your devices in case you misplace them.<br>• Enable two-factor authentication for all applications. | • Don't use unlicensed software.<br>• Don't use old versions of software or applications that don't receive periodic updates.<br>• Don't continue to rely on applications after the trial period has expired. |

## Email — Links and attachments

| Dos: | Don'ts: |
|---|---|
| • Verify the email address of the sender before opening any unsolicited emails.<br>• Scan your email attachments for viruses and malware.<br>• Scan links and use link expanders to determine the true nature of the link before clicking on them.<br>• Even if an email seems legitimate, check for subtle changes in the sender email address or name.<br>• Learn to recognise common phishing techniques, such as messages threatening to shutdown your account, messages trying to create a false sense of urgency, or poorly put together messages.<br>• Hover your mouse over links before you click on them to check if the URL looks legitimate. | • Don't open unsolicited email attachments.<br>• Don't click on short or suspicious URLs sent via email.<br>• Don't get tricked into giving away confidential information.<br>• Don't respond to emails or phone calls asking for confidential information.<br>• Don't forward or reply to junk or spam emails.<br>• Avoid checking emails over public Wi-Fi. |

## Passwords

| Dos: | Don'ts: |
|---|---|
| • Use different passwords for each application and service you use.<br>• Use a password management tool to manage and share your passwords securely.<br>• If you need to share your password with someone, revoke their access as soon as their job is done.<br>• Always store passwords in an encrypted format so it's not easily exploitable.<br>• Regularly update your passwords or use a password management tool that automatically regenerates random passwords periodically. | • Don't share your passwords with people who don't need access to them.<br>• Don't store your passwords in easily accessible places such as public files or handwritten notes.<br>• Don't reuse old passwords.<br>• Don't use dictionary words or easily guessable words (such as pet names, family, friends, etc.) for your passwords. |

## Privacy

| Dos: | Don'ts: |
|---|---|
| • Share the least amount of personal information required.<br>• Search yourself on the internet to check what public information is available about you.<br>• Limit ad tracking on all devices, browsers, and social media channels.<br>• Read the privacy policies of the online services you sign up for. | • Don't ignore unsolicited communications. Report them.<br>• Don't use business devices for personal use.<br>• Don't hoard data you no longer need or use. |