Cyber Security Checklist

The following is our top 20 checklist of key cyber security issues you should consider to help limit the risk and impact of a data breach.

1. Never process a payment or amend existing bank details/frequent payees based on an email request, always follow up an email with a telephone call before making any payments or changing any details.

2. Hover over the email address or check the nick-name to ensure that the sender is who they claim to be.

3. Never click on any unsolicited email links that contain attachments such as.zip or .exe files.

4. Remember – banks and HMRC will never use an email or text message to ask for personal information.

5. Never click on a link in a text message irrespective of who this has been sent from.

6. Keep your software, your operating system and your browser fully up-to-date on all devices, especially Smart Phones. Companies continuously add security updates with every software upgrade they release (also called a patch). Installing these patches immediately will help keep you from becoming infected with new strains of malicious software (“malware”).

7. Always use Multi-Factor Authentication (MFA) to log in to any website or application that you use for banking or investment activity, or that has access to your personal data. MFA is essentially another way—beyond your username and password—to help verify your identity and further safeguard your information.

8. Run a reputable, anti-virus product on your home PC or laptop and keep this up to date. This will also help prevent your device from becoming infected with malware.

9. When processing transactions and/or sending correspondence, avoid using public Wi-Fi hotspots – like the ones at coffee shops, airports, hotels, etc. If you do use a public Wi-Fi hotspot, be sure to use a Virtual Private Network (VPN) so that others can’t intercept your communications. As an alternative, stick to the mobile network and create a personal Wi-Fi hotspot with your phone.

10. Never click on links or open attachments in unsolicited emails or text messages. Doing so may install malware on your device.

11. Avoid using publicly available charging cords to charge your phone. Publicly available outlets and USB ports are generally fine, but avoid using publicly available cords. These can be used to deliver malware.

12. Don’t reuse the same username and password across multiple websites and applications. If you reuse the same username and password and a hacker gains access to one of your accounts, he/she may be able to access your other accounts as well.

13. Create and save bookmarks for the important banking and brokerage websites that you visit often to avoid inadvertently entering your credentials on a fraudulent site.

14. Consider using a password manager. These apps create unique, complex passwords for you and then store those passwords in a cryptographically sound way.

15. Only download applications from Google Play™ or the App Store® and never from a third-party app store. Third-party app stores, or apps that pop up and encourage you to download them, are much more likely to contain malware.

16. Only give applications the permissions they really need. Granting an application access to your photos, location, camera, contacts, etc. makes your data and information available to the application owner.

17. Limit how much information you share on social media, and lock down the privacy settings on your social media accounts. The information you share online could be exploited to gather information for fraud schemes.

18. Shred financial documents before discarding them, as these contain valuable information that could be used by fraudsters. You may wish to leverage online statements and paperless options, like eSign, eDelivery, eAuthorizations and Digital Vault, as these include important security features.

19. Verify that you are using a current and reliable email provider that has basic, built-in security features. Using an older email account that has not incorporated security protections will greatly increase your likelihood of getting malware.

20. If in doubt – DELETE!

For more information around Cyber please speak to a member of our team

The opinions and views expressed in the above articles are those of the author only and are for guidance purposes only. The authors disclaim any liability for reliance upon those opinions and would encourage readers to rely upon more than one source before making a decision based on the information