Compromised Computer Checklist

Cyber Ready Inc.
V1.1

CYBER READY INC.
"PLAN, TRAIN, EXERCISE: YOUR CYBERSECURITY SHIELD."

1) Disconnect the network cable from the compromised computer.
2) The user must change their system password with assistance from the Help Desk or from a clean computer.
3) Communicate to the end user what the process will be to get their computer clean and an estimated time on how long it will take to get it back to them.
4) Remove the compromised computer
    a) Note: the user may need to have a borrowed clean computer delivered to allow them to continue work. Before connecting the borrowed clean computer to the network:
        i) Disable the USB Auto Play feature in Windows 10 to prevent malicious software from executing on the borrowed clean computer (example: https://www.its.qmul.ac.uk/cybersecurity/cyber-awareness-month/turning-off-autorun-in-windows-10/)
        ii) Using the clean borrowed computer, **run a full virus scan (with up-to-date virus definitions) on all internal/external drives** that were connected to the compromised computer.
        iii) Work with the network/server staff to run a full virus scan on all network file shares that were connected to the compromised computer.
        iv) If the virus scans on the internal/external drives and network shares come back clean, the borrowed clean computer can be connected to the network.
5) The tech takes the compromised computer to their lab and performs the following:
    a) Make a copy of the compromised computer Windows Event Viewer logs for future reference.
    b) Start the re-imaging process.
    c) Disable the AutoPlay feature in Windows 10 on the re-imaged computer.
6) Check email client(s) (office and personal) to ensure that email forwarding is turned off.
7) Interview the user to understand if PII data was stored on the compromised computer or internal/external drives connected to the compromised computer.
8) Review network tools (i.e. Darktrace AI) to identify any malicious network activity.

Additional considerations:

- User should consider implementing MFA for other work related online services, as well as home online services.
- After the USB drives have been cleaned and cleared for operation, encrypt the USB drive(s) to avoid a data breach by having a USB drive lost or stolen.
- Provide compromised computer training to the end user.
- Consider using personal Identity Protection monitoring services (e.g. LifeLock, Identity Guard, Bitdefender.