



**Cybersecurity Awareness Month** 

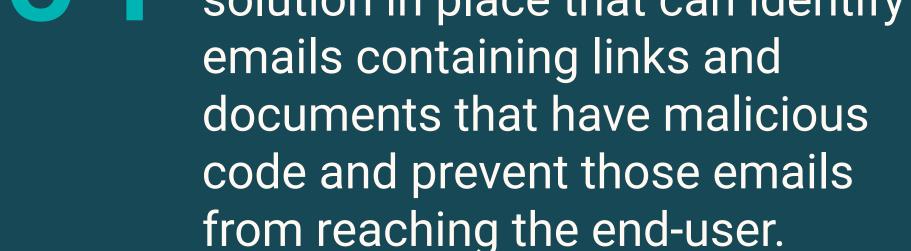
## Protecting Your Organization Against Ransomware

Enable multi-factor authentication on all your internal and external accounts, especially your administrator accounts and all VPN accounts.

Follow the 3-2-1 rule for backups. Have at least three copies of your data. Store the copies on two different media types. Keep one backup copy offsite.

> Avoid using Remote Desktop Protocol (RDP) or SSH publicly. If you must use these, enforce multi-factor authentication.

Have a robust email security solution in place that can identify





Deploy continuous monitoring tools which include next generation endpoint protection and managed detection and response solutions. These tools can detect and stop an attack before it starts and can roll back systems to a prior state. Again, ensure two-factor authentication is enabled on all account.

## Ensure that all your systems have the latest OS updates, security

patches, and third-party application patches. There are several tools available to provide automated patch management.

Provide security awareness
training to your employees
because email is one of the most
frequently used attack vectors for
a ransomware attack. Educating
employees on how to identify
these emails will help to reduce
the potential for a successful
ransomware attack.

www.vlcm.com/cybersecurity