|  |  |
| --- | --- |
|  |  |

***Το λυτρισμικό είναι κακόβουλο λογισμικό που θέτει σε ομηρία τον υπολογιστή και παράλληλα τα δεδομένα προσωπικού χαρακτήρα.*** Συνήθως εισέρχεται στο σύστημα μέσα από κάποιο μήνυμα ηλεκτρονικού ψαρέματος, μέσω τρωτών σημείων του συστήματος, κ.λπ. Το λυτρισμικό κρυπτογραφεί πληροφορίες και, για να μπορέσει το θύμα να ανακτήσει τα δεδομένα, οι κακοποιοί του κυβερνοχώρου απαιτούν ένα σεβαστό ποσό. Ακόμη και αν ο χρήστης πληρώσει το ποσό που του ζητήθηκε, αυτό δεν σημαίνει αυτομάτως ότι θα ανακτήσει τα δεδομένα.  Ρίξτε μια ματιά στο διάγραμμα για να δείτε τι πραγματικά συμβαίνει όταν γίνεται μια τέτοια επίθεση.



**Τι μπορούν να κάνουν οι χρήστες σε αυτή την περίπτωση;**

Υπάρχουν απλά βήματα που μπορούν να σας προστατεύσουν από το λυτρισμικό, όπως:

1. Αποθηκεύετε τα δεδομένα σας σε εφεδρικό σύστημα #BackUp
2. Μην ανοίγετε συνδέσμους που λαμβάνετε από άγνωστες πηγές # Phishing
3. Επικαιροποιείτε τα συστήματά σας #Patch
4. Σε περίπτωση που έχουν προσβληθεί οι συσκευές σας: μην πληρώσετε τα λύτρα που σας ζητούν! #Check www.nomoreransom.org

**Η ασφάλεια στον κυβερνοχώρο αποτελεί κοινή ευθύνη όλων μας**

Ο ευρωπαϊκός μήνας για την ασφάλεια στον κυβερνοχώρο (ECSM) είναι μια εκστρατεία ενημέρωσης που διοργανώνεται σε ολόκληρη την Ευρώπη, κάθε χρόνο τον Οκτώβριο. Στόχος είναι η ενημέρωση των πολιτών και των οργανισμών σχετικά με τις απειλές κατά της ασφάλειας στον κυβερνοχώρο και η προώθηση της ασφάλειας στον κυβερνοχώρο· επίσης, η διάθεση πόρων για την προστασία τους στο διαδίκτυο, μέσω της εκπαίδευσης και της ανταλλαγής ορθών πρακτικών.

# μήνας για την ασφάλεια στον κυβερνοχώρο #ενημέρωση για την ασφάλεια στον κυβερνοχώρο #ηλεκτρονικές δεξιότητες #ασφάλεια στον κυβερνοχώρο