1ο Γυμνάσιο Πεύκων

«Ασφάλεια στο διαδίκτυο»

από τους/τις μαθητές/τριες του Α4 (σχολ. έτος 2023-24)

Flipbook

https://gym-pefkon.thess.sch.gr/activities/healtheducation/202324internetsecurity/index.html

Το κείμενο του FlipBook σε μορφή Pdf παρατίθεται παρακάτω.

Quiz

https://wordwall.net/el/resource/73741971

Σαρώστε για να παίξετε από κινητό ή tablet:

wordwall.net/el/resource/73741971

Προστασία και Ασφάλεια στο Διαδίκτυο

Εργασία των μαθητών Α4 του 1ου Γυμνασίου Πεύκων

Κυβερνοασφάλεια

Καθώς όλο και περισσότερες ψηφιακές πληροφορίες συλλέγονται και μοιράζονται στο διαδίκτυο, η προστασία των πληροφοριών αυτών γίνεται πολύ σημαντική. Η ασφάλεια στον κυβερνοχώρο είναι μία συνεχής προσπάθεια για την προστασία αυτών των δεδομένων από επίδοξους κακόβουλους χρήστες.
Κάποιοι από τους κύριους κινδύνους περιγράφονται παρακάτω

Κακόβουλο Λογισμικό (Malware): Περιλαμβάνει κακόβουλα προγράμματα που μπορούν να προκαλέσουν ζημιά στους υπολογιστές, να καταστρέψουν πληροφορίες ή να κλέψουν προσωπικά δεδομένα. Μερικά από αυτά αναφέρονται παρακάτω

Δούρειος Ίππος (Trojan)

Ο Δούρειος Ίππος είναι μια κατηγορία κακόβουλου λογισμικού που είναι σχεδιασμένος να εισβάλλει στον

υπολογιστή σας χωρίς τη συγκατάθεσή σας. Όταν ενεργοποιείται μπορεί να κάνει διάφορα πράγματα, ανάλογα με τον τρόπο που έχει προγραμματιστεί.

Έτσι μπορεί να κλέψει ευαίσθητες πληροφορίες, να καταστρέψει δεδομένα ή να προσπαθήσει

να έχει πρόσβαση σε άλλους υπολογιστές σε ένα δίκτυο. Οι Δούρειοι Ίπποι συνήθως μεταφέρονται μέσω κακόβουλων ηλεκτρονικών μηνυμάτων, ανεπιθύμητων διαφημίσεων, ή μέσω κακόβουλων ιστοσελίδων.

Spyware

Τα spyware είναι ένα είδος κακόβουλου λογισμικού που σχεδιάζεται για να συλλέγει πληροφορίες και για να παρακολουθεί την δραστηριότητα του χρήστη . Αυτό μπορεί να περιλαμβάνει την καταγραφή του τι πληκτρολογεί ο χρήστης, να συλλέγει πληροφορίες σχετικά με τις ιστοσελίδες που επισκέπτεται, ή ακόμη και να παρακολουθεί τα προσωπικά του δεδομένα.

Τα spyware συνήθως εισέρχονται στον υπολογιστή με διάφορους τρόπους, όπως παράνομες λήψεις λογισμικού, κρυφά προγράμματα εγκατάστασης σε δωρεάν λογισμικό, ή μέσω κενών ασφαλείας στο λειτουργικό σύστημα του υπολογιστή.

Για την προστασία ενός υπολογιστή από τα spyware και τους Δούρειους Ίππους είναι σημαντικό να χρησιμοποιείτε ένα αξιόπιστο λογισμικό ασφαλείας, να ενημερώνετε το λογισμικό σας τακτικά και να είστε προσεκτικοί με τις λήψεις και τα κλικ στο διαδίκτυο.

Adware

Τα adware είναι ένα είδος λογισμικού που δημιουργήθηκε για να εμφανίζει διαφημίσεις στον υπολογιστή του χρήστη.

Οι διαφημίσεις που εμφανίζονται από το adware μπορεί να είναι pop-up παράθυρα ή παράθυρα και banner στις ιστοσελίδες. Πολλές φορές, το adware μπορεί να επιβαρύνει την απόδοση του υπολογιστή.

Για να αντιμετωπίσετε το *adware, θα χρειαστεί να χρησιμοποιήσετε εξειδικευμένο λογισμικό αντι-κακόβουλου* λογισμικού που θα το εντοπίσει και θα το αφαιρέσει από τον υπολογιστή σας. Επίσης, να είστε προσεκτικοί κατά την εγκατάσταση νέου λογισμικού και να διαβάζετε προσεκτικά τις συνθήκες χρήσης και τις άδειες που συνοδεύουν τις εφαρμογές.

Worm

Τα worms είναι ένα είδος κακόβουλου λογισμικού που διαφέρει από τους ιούς και τους Δούρειους Ίππους. Ενώ οι ιοί χρειάζονται έναν φορέα για να μεταφερθούν (όπως ένα αρχείο ή ένα έγγραφο) και οι Δούρειοι Ίπποι παρουσιάζονται ως κανονικά προγράμματα για να εγκατασταθούν, τα worms

μπορούν να αντιγραφούν και να διαδοθούν αυτόνομα μέσω δικτύων, χωρίς την παρέμβαση του χρήστη.

Ένα worm μπορεί να εισβάλλει σε έναν υπολογιστή, να αντιγραφεί στον σκληρό δίσκο και στη συνέχεια να αντιγραφεί σε άλλους υπολογιστές στο ίδιο δίκτυο, χρησιμοποιώντας διάφορους μηχανισμούς εκμετάλλευσης ασφαλείας. Μπορεί να προκαλέσει μεγάλη ζημιά σε μεγάλα δίκτυα, καθώς μπορεί να επηρεάσει εκατοντάδες ή ακόμα και χιλιάδες υπολογιστές σε σύντομο χρονικό διάστημα.

Για την προστασία από τα worms, είναι σημαντικό να χρησιμοποιείτε ενημερωμένο λογισμικό ασφαλείας, να τηρείτε τις βέλτιστες πρακτικές ασφαλείας για δίκτυα, όπως την ενεργοποίηση των τειχών προστασίας πυρήνα (firewalls), και να είστε προσεκτικοί με το πώς αλληλεπιδράτε με τα email και το διαδίκτυο.

Ransomware

Τα ransomware είναι μια μορφή κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα του χρήστη και απαιτεί την πληρωμή λύτρων (ransom) για την αποκρυπτογράφησή τους.

Τα ransomware μπορούν να διαδοθούν μέσω ηλεκτρονικών μηνυμάτων, κακόβουλων συνδέσμων σε ιστοσελίδες, ή

εκμετάλλευσης κενών ασφαλείας σε λογισμικό. Η πληρωμή των λύτρων μπορεί να ζητηθεί να γίνει μέσω κρυπτονομισμάτων ή άλλων ανώνυμων μεθόδων πληρωμής, καθιστώντας την ανίχνευση και την καταδίωξη των υπευθύνων δύσκολη.

Τα ransomware μπορούν να προκαλέσουν σοβαρή ζημιά σε επιχειρήσεις και ιδιώτες, καθώς μπορεί να οδηγήσουν στην απώλεια σημαντικών δεδομένων και στην παράλυση των λειτουργιών ενός οργανισμού.

Για την προστασία από ransomware, είναι σημαντικό να εγκαταστήσετε και να διατηρείτε ενημερωμένο λογισμικό ασφαλείας, να κάνετε αντίγραφα ασφαλείας των δεδομένων σας σε τακτικά χρονικά διαστήματα και να είστε προσεκτικοί με τα email και τα συνημμένα αρχεία που λαμβάνετε.

Botnet

Τα botnet είναι δίκτυα υπολογιστών που έχουν μολυνθεί με κακόβουλο λογισμικό (bot malware) και ελέγχονται από τους δημιουργούς τους, γνωστούς ως botmasters ή bot herders. Οι υπολογιστές που συμμετέχουν

σε ένα botnet, είναι γνωστά ως "bots" ή "zombies" και συνήθως μολύνονται χωρίς τη γνώση των χρηστών τους και εκτελούν εντολές του botmaster.

Τα botnet χρησιμοποιούνται για διάφορους σκοπούς, συμπεριλαμβανομένης της εξαπάτησης και της κλοπής προσωπικών πληροφοριών, της αποστολής μαζικών ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam), της επιτιθέμενης επίθεσης διακοπής υπηρεσιών (DDoS), και άλλων εγκληματικών δραστηριοτήτων.

Για την προστασία από τα botnet, είναι σημαντικό να χρησιμοποιείτε ενημερωμένο λογισμικό ασφαλείας, να αποφεύγετε την πρόσβαση σε κακόβουλες ιστοσελίδες και συνημμένα αρχεία από άγνωστους αποστολείς, και να εφαρμόζετε καλές πρακτικές ασφαλείας σε όλες τις συσκευές και τα δίκτυα που χρησιμοποιείτε.

Keylogger

Το keylogger είναι είδος κακόβουλου λογισμικού σχεδιασμένο για να καταγράφει αυτά που εισάγονται σε έναν υπολογιστή.

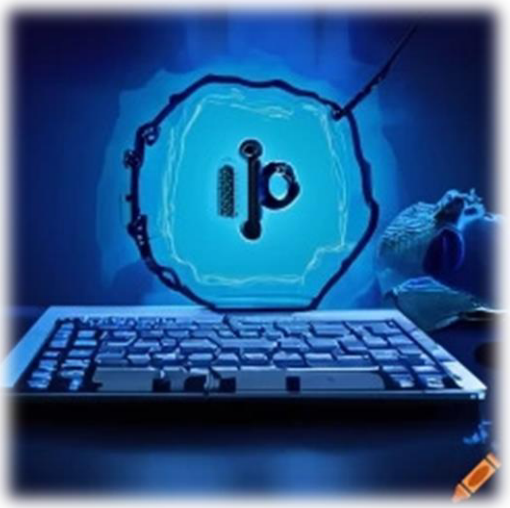
Το keylogger συνήθως εγκαθίσταται στον υπολογιστή του χρήστη μέσω κακόβουλων συνδέσμων, κακόβουλων συνημμένων σε email, είτε μέσω κενών στο λογισμικό

ασφαλείας. Αφού εγκατασταθεί το keylogger παρακολουθεί και καταγράφει όλα όσα πληκτρολογεί ο χρήστης, συλλέγοντας έτσι πληροφορίες όπως κωδικοί πρόσβασης, πιστωτικές κάρτες, και άλλα ευαίσθητα δεδομένα.

Το keylogger χρησιμοποιείται συχνά από κυβερνοεγκληματίες για να προκαλέσουν οικονομική ζημιά ή για να παραβιάσουν την ιδιωτικότητα του χρήστη.

Για την προστασία από keyloggers, είναι σημαντικό να χρησιμοποιείτε αξιόπιστο λογισμικό ασφαλείας, να είστε προσεκτικοί με την περιήγησή σας στο διαδίκτυο και με τα ανοιχτά συνημμένα σε email, και να αποφεύγετε τη χρήση δημόσιων υπολογιστών ή δικτύων και ελεύθερων WIFI για ευαίσθητες δραστηριότητες όπως η τραπεζική.

Phishing



Το phishing είναι μια μορφή κυβερνοεγκληματικής επίθεσης που στοχεύει στην απόκτηση ευαίσθητων πληροφοριών, όπως κωδικοί πρόσβασης, πιστωτικές κάρτες ή άλλα προσωπικά δεδομένα, μέσω παραπλανητικών ηλεκτρονικών μηνυμάτων ή ιστοσελίδων.

Οι επιθέσεις phishing συνήθως γίνονται μέσω νόμιμων υπηρεσιών, όπως τράπεζες, ηλεκτρονικά καταστήματα, κοινωνικά δίκτυα κ.λπ.,

Τα phishing μηνύματα συνήθως περιλαμβάνουν συνδέσμους προς παραπλανητικές ιστοσελίδες που μοιάζουν με τις πραγματικές ιστοσελίδες αυτών που προσποιούνται. Όταν ένα θύμα πατάει στο σύνδεσμο μπορεί να οδηγηθεί σε μια παραπλανητική ιστοσελίδα όπου του ζητείται να καταχωρίσει τις προσωπικές του πληροφορίες.

Η καλύτερη πρακτική για την προστασία από phishing περιλαμβάνει την προσοχή και την επιβεβαίωση της προέλευσης των ηλεκτρονικών μηνυμάτων. Επίσης, πρέπει να αποφεύγετε τα κλικ σε συνδέσμους από ύποπτα email, να επιβεβαιώνετε την ασφάλεια των ιστοσελίδων πριν καταχωρίσετε ευαίσθητες πληροφορίες, και να χρησιμοποιείτε αξιόπιστα λογισμικά ασφαλείας στον υπολογιστή σας.

Spam

Το spam αναφέρεται σε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται σε μεγάλες ποσότητες προς αποδέκτες που δεν τα έχουν ζητήσει. Συνήθως το spam περιέχει

διαφημίσεις για προϊόντα ή υπηρεσίες, αλλά μπορεί επίσης να περιέχει ανεπιθύμητο περιεχόμενο όπως ανεπιθύμητα μηνύματα με παραπλανητικούς συνδέσμους, κακόβουλο λογισμικό ή απάτες (phishing).

Οι αποστολείς του spam συχνά χρησιμοποιούν αυτοματοποιημένους τρόπους αποστολής, όπως λίστες email που έχουν αγοραστεί ή συλλεχθεί από διάφορες πηγές, καθώς και ρομποτικά προγράμματα (bots) για την αποστολή μαζικών μηνυμάτων.

Το spam μπορεί να προκαλέσει ενόχληση και χρονοβόρες διαδικασίες φιλτραρίσματος των μηνυμάτων στα εισερχόμενα του email. Ωστόσο, η πιο σοβαρή ανησυχία σχετίζεται με το περιεχόμενο του spam, το οποίο μπορεί να περιέχει απάτες (phishing) που στοχεύουν στην κλοπή προσωπικών πληροφοριών, κακόβουλο λογισμικό που μπορεί να καταστρέψει ή να κλέψει δεδομένα, ή ακόμη και παραπλανητικά μηνύματα που προσπαθούν να προωθήσουν αμφισβητήσιμες πρακτικές ή προϊόντα.

Για την προστασία από το spam, οι χρήστες συνήθως χρησιμοποιούν λογισμικό φιλτραρίσματος ανεπιθύμητων μηνυμάτων (spam filters) στα email τους και αποφεύγουν τη δημοσίευση της διεύθυνσης email τους σε δημόσια μέρη στο διαδίκτυο.

Μέτρα προστασίας

Υπάρχουν πολλά μέτρα που μπορεί να λάβει κάποιος για να περιηγείται ασφαλώς στο διαδίκτυο. Ανάλογα με το επίπεδο ασφάλειας που επιθυμεί και την ευαισθησία των δεδομένων του, μπορεί να λάβει τα παρακάτω μέτρα:

Ενημέρωση: Ενημερωθείτε για τους κινδύνους του διαδικτύου και μάθετε πώς να τους αντιμετωπίζετε.

Δυνατό Κωδικοί Πρόσβασης: Χρησιμοποιήστε δυνατούς κωδικούς πρόσβασης και διαφορετικούς για κάθε λογαριασμό.

Ενημέρωση Λογισμικού: Βεβαιωθείτε ότι το λογισμικό σας (λειτουργικό σύστημα, προγράμματα περιήγησης, αντιικο κλπ.) είναι ενημερωμένο και έχουν εγκατασταθεί τακτικά ενημερώσεις ασφαλείας.

Χρήση Εξειδικευμένων Εργαλείων: Χρησιμοποιήστε εργαλεία ασφαλείας για προστασία από κακόβουλο λογισμικό.

Αποφυγή Άγνωστων Συνδέσμων: Μην κάνετε κλικ σε συνδέσμους από άγνωστες πηγές ή σε ανεπιθύμητα email.

Χρήση Ασφαλών Συνδέσεων: Αποφύγετε τη χρήση δημόσιων Wi-Fi δικτύων για ευαίσθητες δραστηριότητες όπως online τραπεζικές συναλλαγές.

Η παραπάνω εργασία έγινε στα πλαίσια του **Διαπεριφερειακού θεματικού Δικτύου «Ασφάλεια στο Διαδίκτυο»** από τους μαθητές του τμήματος Α4 του 1ου Γυμνασίου Πεύκων