ΜΟΡΦΕΣ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Αδάμου Εβίτα
Βίτση Γωγώ
Καρανάσου Χριστίνα
Κωταπήτας Γρηγόρης
Μαγγόγιας Παναγιώτης

ΗΛΕΚΤΡΟΝΙΚΌ ΨΑΡΕΜΑ (PHISING)

Το **Phishing** είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, , με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων.

Πώς ξεκίνησε;

Το Phishing ξεκίνησε το 1995 για να πλήξει την τότε μεγαλύτερη διαδικτυακή υπηρεσία επικοινωνίας AOL

Πώς λειτουργεί;

Ο hacker στέλνει ένα e-mail ή άμεσο μήνυμα στο 'θύμα', στο οποίο συστήνεται ως αξιόπιστο πρόσωπο που ανήκει σε κάποια εταιρία ή οργανισμό και ζητά από το θύμα κάποια προσωπικά στοιχεία.

Άλλες τεχνικές Phishing χρησιμοποιούν αναδυόμενα παράθυρα, πολλαπλές καρτέλες ή ακόμα και τη δημιουργία ψεύτικων δημοσίων δικτύων σε αεροδρόμια, ξενοδοχεία και καφετέρειες.

Πώς μπορείτε να εντοπίσετε ένα μήνυμα ψαρέματος;

Οι επιτήδειοι της ηλεκτρονικής απάτης σας πλησιάζουν με ψεύτικα προσχήματα και προσπαθούν να σας πείσουν να κοινοποιήσετε σημαντικές προσωπικές πληροφορίες όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης ή δεδομένα του λογαριασμού σας. Οι απάτες ψαρέματος μπορεί να γίνουν αυτοπροσώπως ή μέσω τηλεφώνου.

Ενδείξεις πως ένα ηλεκτρονικό μήνυμα πιθανόν να είναι πλαστό

Στις απάτες ψαρέματος συνηθίζονται οι γενικές προσφωνήσεις όπως "Αγαπητέ πελάτη" αντί για το όνομά σας. Σας ζητούν να κάνετε κλικ σε κάποιο σύνδεσμο, με φρασεολογία που δίνει την εντύπωση του επείγοντος ή σας ζητούν να επιβεβαιώσετε κάποιες προσωπικές σας πληροφορίες.

ΤΙ ΝΑ ΚΑΝΕΤΕ ΕΑΝ ΠΕΣΕΤΕ ΘΥΜΑ ΑΠΑΤΗΣ ΜΕ ΤΗΝ ΠΙΣΤΩΤΙΚΗ ΣΑΣ ΚΑΡΤΑ.

- Επικοινωνήσετε με τις αρμόδιες αρχές
- Κλείστε όλους τους λογαριασμούς που επηρεάζονται
- Επικοινωνήστε με την πραγματική εταιρεία ή τον οργανισμό εάν πιστεύετε πως δώσατε ευαίσθητες πληροφορίες σε άγνωστη πηγή
- Όταν ανοίξετε νέους λογαριασμούς χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης
- Προσθέστε ειδοποίηση απάτης στους πιστωτικούς λογαριασμούς
- Ζητήστε ένα αντίγραφο της αναλυτικής κατάστασης του λογαριασμού σας και ζητήστε να μην γίνει καμία νέα πίστωση του λογαριασμού χωρίς την έγκριση σας.

Απενεργοποίηση ειδοποιήσεων για ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware)

- Στην επάνω δεξιά γωνία του παραθύρου του προγράμματος περιήγησης, κάντε κλικ στο μενού Chrome .
- Κάντε κλικ στις **Ρυθμίσεις**.
- Κάντε κλικ στην **Εμφάνιση σύνθετων ρυθμίσεων**.
- Στην περιοχή "Απόρρητο", καταργήστε το πλαίσιο "Ενεργοποίηση προστασίας από ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware)".

ΗΛΕΚΤΡΟΝΙΚΌ «ΨΆΡΕΜΑ» ΚΑΙ FACEBOOK

- Όταν ένας χρήστης πέσει θύμα ηλεκτρονικού ψαρέματος, συχνά ο λογαριασμός του αρχίζει να στέλνει αυτόματα μηνύματα ή συνδέσμους σε πολλούς φίλους του. Τα μηνύματα αυτά ή οι σύνδεσμοι είναι συνήθως διαφημίσεις που ζητούν από τους φίλους του χρήστη να δουν βίντεο ή προϊόντα.
- *Αν ο λογαριασμός σας στέλνει αυτόματα ανεπιθύμητα μηνύματα ή συνδέσμους, ασφαλίστε τον. Αν πιστεύετε ότι ο λογαριασμός ενός φίλου σας έχει πέσει θύμα ηλεκτρονικού ψαρέματος, πείτε στο φίλο σας να αλλάξει τον κωδικό πρόσβασής του και να χρησιμοποιήσει στον υπολογιστή του λογισμικό προστασίας από ιούς.*

Να είστε επιφυλακτικοί με:

- Μηνύματα που περιέχουν ορθογραφικά και τυπογραφικά λάθη
- Μηνύματα που ισχυρίζονται ότι περιλαμβάνουν τον κωδικό πρόσβασής σας ως συνημμένο αρχείο
- Μηνύματα που σας ζητούν προσωπικές πληροφορίες
- Μηνύματα που ισχυρίζονται ότι ο λογαριασμός σας θα διαγραφεί ή θα κλειδωθεί αν δεν κάνετε άμεσα κάποια ενέργεια.

Τρόποι για να ελέγξετε αν ένα μήνυμα email προέρχεται πραγματικά από το Facebook

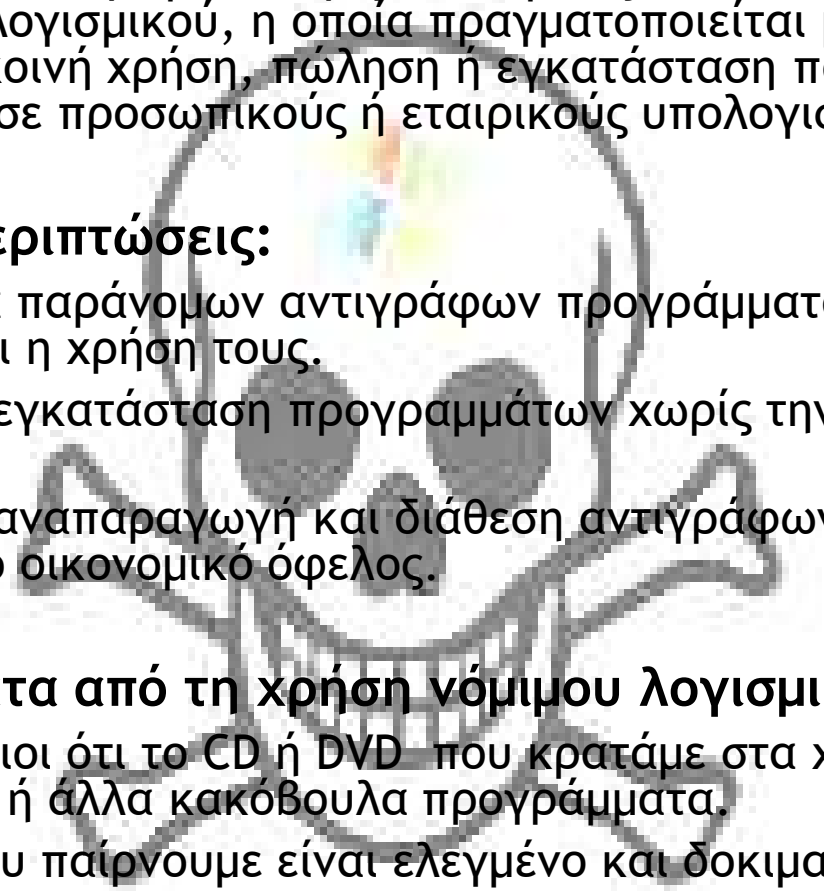
- Κάντε δεξί κλικ στο σύνδεσμο και αντιγράψτε τη διεύθυνση URL
- Επικολλήστε τη διεύθυνση στο πρόγραμμα περιήγησης που χρησιμοποιείτε.
- Βεβαιωθείτε ότι η διεύθυνση αρχίζει με το «www.facebook.com»

Λύσεις

- Υπάρχουσες νομοθεσίες
- Ενημέρωση του κοινού
- Τεχνική Αντιμετώπιση

ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ

Ως πειρατεία λογισμικού ορίζεται η μη εξουσιοδοτημένη αντιγραφή ή η διανομή λογισμικού, η οποία πραγματοποιείται με την , λήψη, αντιγραφή, κοινή χρήση, πώληση ή εγκατάσταση πολλαπλών αντιγράφων σε προσωπικούς ή εταιρικούς υπολογιστές.



Βασικές περιπτώσεις:

- Η δημιουργία παράνομων αντιγράφων προγράμματος από το αυθεντικό και η χρήση τους.
- Η παράνομη εγκατάσταση προγραμμάτων χωρίς την άδεια του δημιουργού.
- Η παράνομη αναπαραγωγή και διάθεση αντιγράφων προγραμμάτων με κίνητρο το οικονομικό όφελος.

Πλεονεκτήματα από τη χρήση νόμιμου λογισμικού

1. Είμαστε βέβαιοι ότι το CD ή DVD που κρατάμε στα χέρια μας δεν περιέχει ιούς ή άλλα κακόβουλα προγράμματα.
2. Το προϊόν που παίρνουμε είναι ελεγμένο και δοκιμασμένο.
3. Μας παρέχονται τα απαραίτητα εγχειρίδια χρήσης, για να μάθουμε να χρησιμοποιούμε σωστά το νέο πρόγραμμα.
4. Έχουμε τεχνική υποστήριξη από τους κατασκευαστές.
5. Μπορούμε να το χρησιμοποιήσουμε νόμιμα, για να παράγουμε και εμείς με τη σειρά μας τη δική μας πνευματική εργασία.

ΚΊΝΔΥΝΟΙ ΑΠΌ ΠΕΙΡΑΤΕΊΑ ΛΟΓΙΣΜΙΚΟΎ

- Το πειρατικό λογισμικό μπορεί να προκαλέσει ολικές βλάβες του υπολογιστή σας.
- Το πλαστό λογισμικό μπορεί να περιέχει spyware που φορτώνεται στον υπολογιστή σας και αναφέρει προσωπικά δεδομένα χωρίς να το γνωρίζετε, όπως αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών, κωδικούς πρόσβασης και βιβλία διευθύνσεων.
- Οι κυβερνοκλέφτες ανακαλύπτουν κατά περιόδους ευπάθειες σε λογισμικό και οι προμηθευτές λογισμικού παρέχουν διορθωτικές εκδόσεις που αντιμετωπίζουν την ευπάθεια.
- Ένας πωλητής που προτείνει να παραβιάσετε το νόμο ίσως να μη σταματήσει στο πειρατικό λογισμικό.

Πως να αποφύγετε τη πειρατεία λογισμικού

-Αγοράζετε λογισμικό μόνο από αξιόπιστες εταιρείες

-Όταν κάνετε αγορές online, να βεβαιώνεστε ότι η ιστοσελίδα είναι νομότυπη.

-Πριν δώσετε στοιχεία πιστωτικής κάρτας, ελέγξτε τη διεύθυνση URL της ιστοσελίδας

- Αν σας φαίνεται ότι μια τιμή φαίνεται πολύ καλή για να είναι αληθινή, μάλλον έτσι είναι

- Αν το λογισμικό σας καταφθάσει σε μια λευκή θήκη ή σε έναν απλό φάκελο, πιθανότατα είναι πλαστό.

ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Κάποιες από τις πιο συχνές ηλεκτρονικές απάτες στο διαδίκτυο είναι:

- Pharming
- Scam
- Blog
- Διαδικτυακός τζόγος

PHARMING

Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name) που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη, η οποία όμως μοιάζει πανομοιότυπη με τη γνήσια.

SCAM

Σε γενικές γραμμές οι απάτες που είναι γνωστές με τον όρο «scam» αφορούν κάποια συναλλαγή που για να ολοκληρωθεί χρειάζεται κάποια χρήματα από το υποψήφιο θύμα - παραλήπτη του παραπλανητικού μηνύματος. Ωστόσο, το θύμα δεν παραλαμβάνει ποτέ τα προσφερόμενα ανταλλάγματα.

BLOG

Η πρακτική του blogging, η τήρηση προσωπικού ημερολογίου στο Διαδίκτυο, μεγαλώνει δραματικά— ειδικά ανάμεσα στους έφηβους, οι οποίοι ορισμένες φορές διατηρούν ημερολόγια blog χωρίς να το γνωρίζουν οι γονείς ή οι κηδεμόνες τους.

ΔΙΑΔΙΚΤΥΑΚΟΣ ΤΖΟΓΟΣ

Ποιά είναι η διαφορά ανάμεσα στις τοποθεσίες παιχνιδιών και τις τοποθεσίες τυχερών παιχνιδιών;

Οι κυριότερες διαφορές μεταξύ των τύπων των ιστοσελίδων είναι οι εξής:

- Οι τοποθεσίες παιχνιδιών συνήθως περιέχουν παιχνίδια με κάρτες, πίνακες, λέξεις, arcade ή παζλ, με αυτόματη παρακολούθηση και προβολή του σκορ.
- Δεν γίνεται ανταλλαγή χρημάτων, αληθινών ή ψεύτικων. Οι τοποθεσίες τυχερών παιχνιδιών μπορούν να περιέχουν σενάρια, στα οποία οι άνθρωποι κερδίζουν ή χάνουν κάποιο τεχνητό νόμισμα. Οι τοποθεσίες Τζόγου συνήθως αφορούν το κέρδος ή την απώλεια αληθινών χρημάτων.

Πώς να αναγνωρίζετε τις απάτες

- Νέες απάτες φαίνεται να εμφανίζονται κάθε μέρα και μπορεί να περιλαμβάνουν τα ακόλουθα:
- Μηνύματα με κινδυνολογίες και απειλές για κλείσιμο του λογαριασμού.
- Υποσχέσεις για χρήματα με μικρή ή καθόλου προσπάθεια.
- Προσφορές που ακούγονται πολύ καλές για να είναι αληθινές.
- Αιτήσεις για δωρεές σε φιλανθρωπικές οργανώσεις μετά από μια καταστροφή.
- Γραμματικά και ορθογραφικά λάθη.

Τι να κάνετε αν νομίζετε ότι έχετε πέσει θύμα μιας απάτης

- Αλλάξτε τους κωδικούς πρόσβασης ή κωδικούς PIN για όλες τους online λογαριασμούς που νομίζετε ότι μπορεί να έχουν τεθεί σε κίνδυνο.
- Ζητήστε ειδοποιήση συναλλαγών για την πιστωτική κάρτα σας μέσω της τράπεζας. Επικοινωνήστε με την τράπεζά ή οικονομικό σύμβουλο σας, αν δεν είστε σίγουροι για το πώς να το κάνετε αυτό.
- Μην ακολουθείτε links από ύποπτα μήνυμα ηλεκτρονικού ταχυδρομείου.
- Αν γνωρίζετε όλους τους λογαριασμούς που παραβιάστηκαν, κλείστε τους.
- Ελέγχετε τακτικά τις τραπεζικές καταθέσεις και πιστωτικές κάρτες σας κάθε μήνα για ανεξήγητες αλλαγές ή χρεώσεις.

ΔΙΑΚΙΝΗΣΗ ΠΟΡΝΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΥ

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Ο κοινός παρανομαστής είναι οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή ή και καρτούν.

Μορφές:

1. Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
2. Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο
3. Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες

ΤΙ ΕΊΝΑΙ ΤΟ ΚΥΚΛΩΜΑ ΠΑΙΔΟΦΙΛΙΑΣ

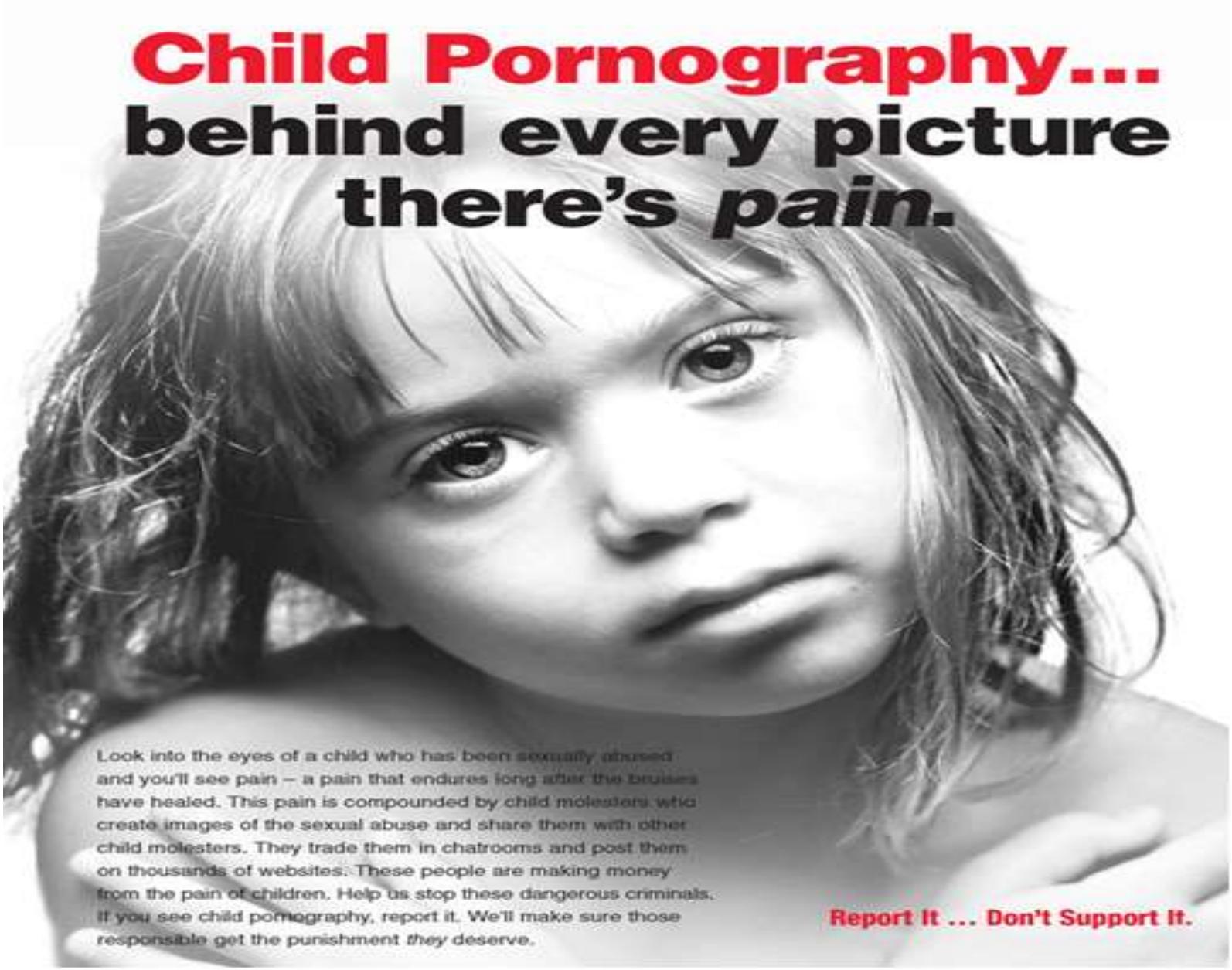
Ένα κύκλωμα παιδοφιλίας είναι μια ομάδα ανθρώπων που εργάζονται μαζί μέσω Διαδικτύου σε διαφορετικές χώρες και υπό διαφορετικά νομοθετικά πλαίσια, με σκοπό τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Μπορεί επίσης να γίνεται και ανταλλαγή εμπειριών και γνώσεων ως προς την αποφυγή ανίχνευσης και το σχεδιασμό εγκληματικών ενεργειών εις βάρος παιδιών.

ΤΡΟΠΟΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ Η ΧΡΗΣΗ ΤΟΥΣ ΣΤΗΝ ΔΙΑΝΟΜΗ ΠΑΡΑΝΟΜΟΥ ΠΟΡΝΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΎ

1. Δωμάτιο Συνομιλίας
2. Στιγμιαίο Μήνυμα (IM)
3. Ηλεκτρονικό ταχυδρομείο (e-mail)
4. Ηλεκτρονικές ομάδες (e-groups)
5. Κατάλογοι ηλεκτρονικών διευθύνσεων
6. Ομάδες πληροφόρησης
7. Πίνακας δελτίων (BBS)

Οδηγίες προς τους γονείς

- Να ενημερωθούν για τους κινδύνους που κρύβει η ανεπιτήρητη πλοήγηση των παιδιών στο Internet.
- Να εξοικειωθούν και εκείνοι στη χρήση του διαδικτύου, για να μπορούν να μιλούν την ίδια γλώσσα με τα παιδιά τους.
- Να θεσπίσουν κανόνες στην πρόσβαση στο Internet, όπως:
- Να μην επιτρέπουν στα παιδιά τους να δίνουν πληροφορίες για προσωπικά στοιχεία, δηλαδή ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο, επάγγελμα γονιών, οικογενειακή κατάσταση, αριθμό πιστωτικής κάρτας.
- Να απαγορεύεται στα παιδιά να συναντηθούν με άτομο που γνώρισαν στο διαδίκτυο, χωρίς την ενημέρωση και άδεια των γονιών.
- Να μη στέλνουν φωτογραφίες σε γνωριμίες από το Internet.


Child Pornography...
behind every picture
there's pain.
Look into the eyes of a child who has been sexually abused and you'll see pain – a pain that endures long after the bruises have healed. This pain is compounded by child molesters who create images of the sexual abuse and share them with other child molesters. They trade them in chatrooms and post them on thousands of websites. These people are making money from the pain of children. Help us stop these dangerous criminals. If you see child pornography, report it. We'll make sure those responsible get the punishment they deserve.
Report It ... Don't Support It.

ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

Με τον όρο **βρώμικο χρήμα**, ή **μαύρο χρήμα** και ευρύτερα **μαύρα**, καθιερώθηκε να χαρακτηρίζεται, περισσότερο δημοσιογραφικά, οποιοδήποτε είδος εσόδου από παράνομη πράξη, ή ακόμη και έσοδο από νόμιμη πράξη το οποίο στη συνέχεια δεν δηλώνεται, κατά παράβαση της υφιστάμενης φορολογικής νομοθεσίας. Και στις δύο περιπτώσεις ανάγεται σε οικονομικό έγκλημα.

ΤΡΟΠΟΙ

- *Ψηφιακά νομίσματα*
- *Online Gaming*
- *Παραπλανητικά e-mail*
- *Προσφορά εργασίας από το σπίτι*
- *Online στοιχιματικές υπηρεσίες*

ΟΙ ΤΕΧΝΙΚΕΣ ΞΕΠΛΥΜΑΤΟΣ ΧΡΗΜΑΤΟΣ

Θα μπορούσαμε να χρησιμοποιήσουμε κάποιες εκτιμήσεις των τελωνιακών υπηρεσιών των Η.Π.Α. προκειμένου να απεικονίσουμε τις κυριότερες τεχνικές που χρησιμοποιούνται διεθνώς για την νομιμοποίηση των εσόδων από εγκληματικές δραστηριότητες και στις τρεις φάσεις που προαναφέραμε.

ΤΟΠΟΘΕΤΗΣΗ

- Ψευδής παρουσίαση ή απόκρυψη της πραγματικής προέλευσης των δικαιούχων και χρησιμοποίηση εταιριών- βιτρίνα, διατραπεζικές συναλλαγές και εξαιρέσεις από την υποχρέωση αναφοράς και εξακρίβωσης ταυτότητας.
- Μέθοδος του μυρμηγκιού
- Συνεργία από το εσωτερικό κάποιου χρηματοπιστωτικού οργανισμού
- διασυνοριακή λαθραία φυσική μεταφορά χρημάτων μέσω πλοίων, αεροπλάνων, απεσταλμένων συσκευασμένα ως εμπορεύματα
- Απόκτηση υλικών αντικειμένων (ακίνητα, πολύτιμα κοσμήματα και μέταλλα, πλοία, αυτοκίνητα, αεροπλάνα) ή χρηματιστηριακών τίτλων, επιταγών και άλλων τραπεζογραμματίων.

ΣΥΣΣΩΡΕΥΣΗ

- Ηλεκτρονική μεταφορά κεφαλαίων μέσω διαδικτύου
- Μετατροπή χρήματος σε άλλες χρηματοοικονομικές μορφές
- Πώληση ή εξαγωγή περιουσιακών στοιχείων
- Παραποίηση εξαγωγικών και εισαγωγικών εγγράφων30

ΟΛΟΚΛΗΡΩΣΗ

- Εταιρίες βιτρίνα

ΔΙΑΔΙΚΤΥΑΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες»

Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

1. Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.
2. Οι ενέργειες τους δύσκολα εντοπίζονται.
3. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
4. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρώντας την ανωνυμία του.

ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

Ο όρος Διαδικτυακός εκφοβισμός (cyberbullying) αφορά τον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από συνομηλίκους τους.

ΜΟΡΦΕΣ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΚΦΟΒΙΣΜΟΥ

- Επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων
- Παρέμβαση και παρενόχληση οποιασδήποτε δραστηριότητας του ατόμου
- Δημιουργία ψεύτικων διαδικτυακών προφίλ
- Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- Αποστολή φωτογραφιών του ατόμου ή άλλου είδους μαγνητοσκοπημένου υλικού
- Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες
- Αποστολή απειλητικών μηνυμάτων σε άλλα άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου


STOP
BULLYING
NOW
STAND UP • SPEAK OUT

ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΚΦΟΒΙΣΜΟΥ

1. Αγνόηση ενοχλητικών μηνυμάτων, σε περίπτωση ωστόσο απειλών συνιστάται αναφορά των μηνυμάτων και λήψη προληπτικών μέτρων
2. Αποκλεισμός του αποστολέα των απειλητικών μηνυμάτων
3. Αναφορά της περίστασης στον γονέα ή κηδεμόνα
4. Αναφορά του περιστατικού στην Αστυνομία είτε σε κάποια αρμόδια υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος

ΕΙΔΗ ΠΑΡΑΤΗΡΗΤΩΝ ΣΤΟΝ ΔΙΑΔΙΚΤΥΑΚΟ ΕΚΦΟΒΙΣΜΟ

Όπως ακριβώς και στον σχολικό εκφοβισμό έτσι και στον διαδικτυακό καταγράφονται κυρίως δύο είδη παρατηρητών (bystanders).

- Στην πρώτη κατηγορία ανήκουν οι επιβλαβείς για το θύμα παρατηρητές, καθώς επιδοκιμάζουν την συμπεριφορά του θύτη ενισχύοντας έτσι την ένταση του εκφοβιστικού γεγονότος
- Σε αντίθεση με την πρώτη κατηγορία, οι βοηθοί παρατηρητές αντιδρούν άμεσα και ενεργά στο συμβάν του διαδικτυακού εκφοβισμού.


You Loser

ΕΥΧΑΡΙΣΤΟΥΜΕ ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ!

Για προβολή πατήστε video