ProDefence

Cyber Security Services

"ΚΛΙΚ ΕΔΩ, ΤΩΡΑ ΕΚΕΙ""

ΠΥΡΕΤΟΣ ΕΠΕΝΔΥΤΩΝ

Το άρθρο στοχεύει να διερευνήσει λεπτομερώς αυτές τις ύπουλες τακτικές, να κατανοήσει πώς λειτουργούν αυτοί οι εγκληματίες και να περιγράψει αποτελεσματικά μέτρα για την πρόληψη και την καταπολέμηση αυτών των απατών. Θα παρέχουμε βασικές συμβουλές και στρατηγικές τόσο για τα σημερινά όσο και για τα δυνητικά θύματα και τα χρηματοπιστωτικά ιδρύματα για την ενίσχυση της άμυνας ενάντια σε αυτές τις ολοένα και πιο εκλεπτυσμένες κυβερνοεπιθέσεις. Με την ευαισθητοποίηση και την εφαρμογή ισχυρών πρακτικών ασφαλείας, μπορούμε να ελπίζουμε ότι θα προστατεύσουμε καλύτερα τόσο τους οικονομικούς μας πόρους όσο και τις προσωπικές πληροφορίες.

Alexandru Angheluș

Ιδιαίτερες ευχαριστίες για την υποστήριξη του εγγράφου

Zaborilă Florin Ionuț – Αξιωματικός στο IPJ Iași

Τμήμα Διερεύνησης Εγκλημάτων Υπολογιστών

Το "**INVESTOR FEVER"** ορίζει τη συμπεριφορά των ανθρώπων που, από απλοί χρήστες της τεχνολογίας και του Διαδικτύου, γίνονται μεγάλοι επενδυτές μέσω αυτών, αγνοώντας όλα όσα έχουν αποκτήσει από μια ορισμένη ηλικία: διαίσθηση, επιλεκτική εμπιστοσύνη, καχυποψία, σχετικές πληροφορίες κ.λπ.

Από τις καταθέσεις των θυμάτων μπορείτε να μάθετε τι βίωσαν κατά τη διάρκεια αυτής της περιόδου της ζωής τους:

- «Επένδυσα 20.000 ευρώ και έχω ήδη κέρδος 150.000, αλλά δεν μπορώ να το βγάλω. Ο σύμβουλος λέει ότι οι ισοπαλίες επηρεάζουν τις ακόλουθες συναλλαγές μακροπρόθεσμα.
- "Μετά από 10.000 ευρώ που επενδύθηκαν έλαβα το 10% του ποσού, αλλά αν συνεχίσω να επενδύω μετά από 12 μήνες μπορώ να εξαγάγω το 45% του ποσού από τον λογαριασμό".
- «Έχασα 7500 ευρώ με επενδύσεις και η αστυνομία μου είπε ότι ήταν ανασκολοπισμένο... Μερικοί ανόητοι, δεν ξέρουν ότι έτσι είναι στην επένδυση, χάνετε ... Ακόμα κερδίζεις, γιατί αυτό μου είπε ο σύμβουλος από την αρχή».
- «Άρχισα να στέλνω χρήματα και αγόρασα μετοχές, αλλά δεν το λέω σε κανέναν... ότι ξέρεις πώς είναι οι άνθρωποι, ζηλιάρης».
- «Η Τράπεζα είπε ότι πίσω από την επένδυση υπήρχε ένας τσαρλατάνος που με ξεγέλασε, αλλά δεν το πιστεύω! Αυτός ο άνθρωπος και εγώ μιλήσαμε πολύ, μου είπε για την οικογένειά του, είχε επίσης προβλήματα, ήταν αναστατωμένος που δούλευε πολλές ώρες».

1. Εισαγωγή
    - Εξέλιξη της οικονομικής απάτης
2. Ψεύτικη επενδυτική απάτη
    - Μέθοδοι εξαπάτησης
    - Παραδείγματα απάτης
3. Εφαρμογές που χρησιμοποιούνται και πρόσβαση σε τραπεζικούς λογαριασμούς
    - Επικίνδυνες τακτικές εγκατάστασης εφαρμογών
    - Κίνδυνοι που σχετίζονται με εφαρμογές που χρησιμοποιούνται
4. Απεικόνιση του συστήματος απάτης
    - Η πολυπλοκότητα της διαδικασίας απάτης
    - Ανάλυση των σταδίων οικονομικής απάτης
5. Πρόληψη και προστασία των θυμάτων
    - Προειδοποιητικά σημάδια πιθανής απάτης
    - Συμβουλές πρόληψης
6. Ο ρόλος των χρηματοπιστωτικών ιδρυμάτων
    - Μέτρα ασφάλειας και παρακολούθησης
    - Εκπαίδευση πελατών στον τομέα της ασφάλειας στον κυβερνοχώρο
7. Σχέδιο αντιμετώπισης συμβιβασμών
    - Άμεση δράση μετά τον εντοπισμό απάτης
    - Ανάκτηση ζημιών και εξασφάλιση λογαριασμών
8. Συμπέρασμα
    - Η σημασία της ευαισθητοποίησης και της πρόληψης
9. Δώρο
    - Εν εξελίξει εκστρατείες απάτης
    - Πηγές και περαιτέρω ανάγνωση

1. Εισαγωγή

Εξέλιξη της οικονομικής απάτης

Η απάτη, με την ευρύτερη έννοιά της, αναφέρεται σε οποιαδήποτε σκόπιμη πράξη εξαπάτησης που εκτελείται για προσωπικό όφελος ή για να προκαλέσει βλάβη σε κάποιον άλλο. Είναι μια έννοια που εκδηλώνεται σε πολλαπλές μορφές, που κυμαίνονται από απλή εξαπάτηση έως πολύπλοκα σχήματα που περιλαμβάνουν τη χειραγώγηση συστημάτων ή διαδικασιών.

Όταν μιλάμε για οικονομική απάτη, αναφερόμαστε σε εκείνες τις πράξεις εξαπάτησης που αποσκοπούν στην απόκτηση παράνομων οικονομικών οφελών. Μπορεί να περιλαμβάνει τη χειραγώγηση ή την εκμετάλλευση χρηματοπιστωτικών συστημάτων, όπως οι τράπεζες ή οι κεφαλαιαγορές, ή μπορεί να εμπλέκει άμεσα μεμονωμένα θύματα μέσω απάτης και εξαπάτησης. Η οικονομική απάτη περιλαμβάνει ένα ευρύ φάσμα παράνομων δραστηριοτήτων, όπως κλοπή ταυτότητας, απάτη με πιστωτικές κάρτες, συστήματα Ponzi και άλλους τύπους απάτης που αποσκοπούν στην απόκτηση χρημάτων, αγαθών ή υπηρεσιών χωρίς νόμιμο δικαίωμα σε αυτά.

Απάτη που διαπράττεται μέσω συστημάτων πληροφορικής και ηλεκτρονικών μέσων πληρωμήςΠοινικός Κώδικας

Σύμφωνα με τον Ποινικό Κώδικα, οι απάτες αυτές αναφέρονται στο ειδικό μέρος, το οποίο αναφέρεται στα «Εγκλήματα κατά της ιδιοκτησίας», κεφάλαιο IV, άρθρα 249-250-251 και τιμωρείται με φυλάκιση.

Απάτη στον υπολογιστή - Άρθρο 249 - Εισαγωγή, τροποποίηση ή διαγραφή δεδομένων υπολογιστή, περιορισμός της πρόσβασης σε αυτά τα δεδομένα ή παρεμπόδιση με οποιονδήποτε τρόπο της λειτουργίας ενός συστήματος υπολογιστή, με σκοπό την απόκτηση υλικού οφέλους για τον εαυτό του ή για άλλο, εάν έχει προκληθεί ζημία σε ένα άτομο, τιμωρείται με φυλάκιση από 2 έως 7 έτη.

Η δόλια εκτέλεση χρηματοοικονομικών πράξεων - άρθρο 250 - Εκτέλεση ανάληψης μετρητών, φόρτωσης ή τηλεφόρτωσης μέσου ηλεκτρονικού χρήματος ή μεταφοράς χρηματικών ποσών, με τη χρήση, χωρίς τη συγκατάθεση του κατόχου, μέσου ηλεκτρονικής πληρωμής ή στοιχείων ταυτοποίησης που επιτρέπουν τη χρήση του, τιμωρείται με φυλάκιση από 2 έως 7 έτη.

- Η εκτέλεση μιας από τις πράξεις που αναφέρονται στην παράγραφο 1 τιμωρείται με την ίδια ποινή. (1) με μη εξουσιοδοτημένη χρήση οποιωνδήποτε δεδομένων ταυτοποίησης ή με τη χρήση πλασματικών δεδομένων ταυτοποίησης.

- Η μη εξουσιοδοτημένη διαβίβαση σε άλλο πρόσωπο οποιωνδήποτε στοιχείων ταυτοποίησης, προκειμένου να πραγματοποιηθεί μία από τις πράξεις που προβλέπονται στην παρ. (1), τιμωρείται με φυλάκιση από ένα έως 5 έτη.

Αποδοχή δολίως εκτελεσθεισών χρηματοοικονομικών πράξεων – Άρθρο 251 – Αποδοχή ανάληψης μετρητών, φόρτωσης ή τηλεφόρτωσης μέσου ηλεκτρονικού χρήματος ή μεταφοράς χρηματικών ποσών, εν γνώσει του γεγονότος ότι πραγματοποιείται με τη χρήση παραποιημένου μέσου ηλεκτρονικής πληρωμής ή χρησιμοποιείται χωρίς τη συγκατάθεση του κατόχου του, τιμωρείται με φυλάκιση από ένα έως 5 έτη.

- Η αποδοχή μιας από τις πράξεις που αναφέρονται στην παράγραφο 1 τιμωρείται με την ίδια ποινή. (1), εν γνώσει του γεγονότος ότι πραγματοποιείται μέσω μη εξουσιοδοτημένης χρήσης οποιωνδήποτε δεδομένων ταυτοποίησης ή μέσω της χρήσης πλασματικών δεδομένων ταυτοποίησης.

Τις τελευταίες δεκαετίες, με την πρόοδο της τεχνολογίας και τη μαζική ψηφιοποίηση των χρηματοπιστωτικών υπηρεσιών, έχουμε γίνει μάρτυρες μιας σημαντικής μεταμόρφωσης στη φύση και την πολυπλοκότητα της οικονομικής απάτης. Αυτή η εξέλιξη αντικατοπτρίζει όχι μόνο τις αλλαγές στα εργαλεία και τις μεθόδους που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου, αλλά και τη συνεχή προσαρμογή σε νέα περιβάλλοντα και συμπεριφορές χρηστών στον ψηφιακό χώρο.

Στο παρελθόν, η οικονομική απάτη συχνά περιοριζόταν σε πιο άμεσες και λιγότερο εξελιγμένες τακτικές, όπως η κλοπή ταυτότητας μέσω παραδοσιακών μεθόδων ή οι απάτες ταχυδρομικών παραγγελιών. Ωστόσο, στην εποχή του διαδικτύου και της πανταχού παρούσας συνδεσιμότητας, οι εγκληματίες έχουν αρχίσει να εκμεταλλεύονται το διαδικτυακό περιβάλλον για να αναπτύξουν συστήματα που είναι πολύ πιο περίπλοκα και δύσκολο να εντοπιστούν.

Η σύγχρονη οικονομική απάτη βασίζεται σε μια ποικιλία προηγμένων ψηφιακών τεχνικών. Από το ηλεκτρονικό ψάρεμα (phishing) και την κοινωνική μηχανική έως το κακόβουλο λογισμικό και τις εξελιγμένες κυβερνοεπιθέσεις, οι εγκληματίες έχουν στη διάθεσή τους ένα ευρύ φάσμα εργαλείων για να χειραγωγήσουν, να εξαπατήσουν και να κλέψουν από τα θύματά τους. Αυτές οι μέθοδοι δεν είναι μόνο πιο αποτελεσματικές, αλλά επιτρέπουν επίσης την ανωνυμία, αυξάνοντας έτσι το εύρος και τον αντίκτυπο των επιθέσεων.

Μια ιδιαιτερότητα της σημερινής οικονομικής απάτης είναι η ικανότητα των εγκληματιών να προσαρμόζονται γρήγορα στις νέες τεχνολογίες και τάσεις. Στο πλαίσιο ενός ολοένα και πιο συνδεδεμένου κόσμου, όπου όλο και περισσότερες συναλλαγές πραγματοποιούνται στο διαδίκτυο, οι εγκληματίες έχουν αναπτύξει την ικανότητα να εκμεταλλεύονται γρήγορα οποιαδήποτε ευπάθεια. Αυτό περιλαμβάνει τη χρήση των μέσων κοινωνικής δικτύωσης για τη διάδοση ψεύτικων επενδυτικών σχεδίων, θέτοντας σε κίνδυνο την ασφάλεια των εφαρμογών για κινητά για μη εξουσιοδοτημένη πρόσβαση σε τραπεζικούς λογαριασμούς, ακόμη και την εκμετάλλευση αναδυόμενων τεχνολογιών όπως τα κρυπτονομίσματα και το blockchain για την επινόηση νέων τύπων απάτης.

Αυτή η συνεχώς εξελισσόμενη χρηματοπιστωτική απάτη σημαίνει ότι τόσο οι καταναλωτές όσο και τα χρηματοπιστωτικά ιδρύματα πρέπει να επαγρυπνούν συνεχώς και να προσαρμόζονται στις νέες απειλές. Η εκπαίδευση και η ευαισθητοποίηση είναι ζωτικής σημασίας, όπως και οι επενδύσεις σε συστήματα κυβερνοασφάλειας και παρακολούθησης συναλλαγών. Κατανοώντας την εξέλιξη αυτών των απατών, μπορούμε να αναπτύξουμε αποτελεσματικότερες στρατηγικές για την πρόληψη και την καταπολέμησή τους.

2. Ψεύτικη επενδυτική απάτη

Μέθοδοι εξαπάτησης

Η ψευδής επενδυτική απάτη αποτελεί μείζονα απειλή στον σύγχρονο χρηματοπιστωτικό κόσμο, επηρεάζοντας τόσο τους μεμονωμένους επενδυτές όσο και ορισμένες φορές τις χρηματοπιστωτικές αγορές μεγάλης κλίμακας. Αυτά τα συστήματα εξαπάτησης έχουν σχεδιαστεί για να φαίνονται όσο το δυνατόν πιο πειστικά και κερδοφόρα, χρησιμοποιώντας διάφορες μεθόδους για να δελεάσουν και να χειραγωγήσουν τα θύματα.

Παραπλανητικές διαφημίσεις: Αυτή η τακτική είναι ιδιαίτερα αποτελεσματική λόγω της ευρείας και εύκολης πρόσβασης στο ευρύ κοινό μέσω διαδικτυακών πλατφορμών και κοινωνικών δικτύων. Οι διαφημίσεις μπορούν να έχουν τη μορφή εντυπωσιακών πανό, χορηγούμενων αναρτήσεων ή ακόμα και εξατομικευμένων προτάσεων. Η χρήση ψευδών μαρτυριών ή η εμπλοκή δημόσιων προσώπων, είτε μέσω μη εξουσιοδοτημένης χρήσης των εικόνων τους είτε μέσω ψευδών συνειρμών, αποσκοπεί στη δημιουργία αίσθησης νομιμότητας και εμπιστοσύνης. Αυτό μπορεί να δυσκολέψει τους επενδυτές να διακρίνουν μεταξύ γνήσιων και ψευδών ευκαιριών.

Δόλια μηνύματα ηλεκτρονικού ταχυδρομείου και μηνύματα: Οι εγκληματίες χρησιμοποιούν συχνά μηνύματα ηλεκτρονικού ταχυδρομείου και απευθείας μηνύματα για να επικοινωνήσουν με πιθανά θύματα. Αυτά τα μηνύματα είναι συχνά καλογραμμένα και φαίνεται να προέρχονται από νόμιμα χρηματοπιστωτικά ιδρύματα ή αξιόπιστους συμβούλους. Ο στόχος είναι να κερδηθεί η εμπιστοσύνη των θυμάτων και να τα κάνουν να αποκαλύψουν προσωπικές πληροφορίες ή να επενδύσουν σε ψεύτικα συστήματα.

Ψεύτικοι ιστότοποι: Οι ιστότοποι που δημιουργούνται για την υποστήριξη αυτών των ψεύτικων συστημάτων δημιουργούνται συχνά με υψηλό βαθμό επαγγελματισμού. Μπορούν να περιλαμβάνουν ψεύτικες κριτικές, εντυπωσιακά γραφήματα, ακόμη και προσομοιωμένα συστήματα συναλλαγών για να παρέχουν μια εμφάνιση αυθεντικότητας και επιτυχίας. Αυτοί οι ιστότοποι μπορεί να είναι δύσκολο να διακριθούν από τους νόμιμους, καθιστώντας τους επικίνδυνους για τους επενδυτές.

Πίεση χρόνου: Οι τακτικές πίεσης χρόνου παίζουν με την ανθρώπινη ψυχολογία, δημιουργώντας μια αίσθηση επείγοντος που μπορεί να αναγκάσει τα θύματα να δράσουν γρήγορα χωρίς να έχουν χρόνο να αναλύσουν λεπτομερώς την κατάσταση. Οι εγκληματίες μπορεί να ισχυριστούν ότι η προσφορά είναι περιορισμένη χρονικά ή ότι οι επενδυτικές ευκαιρίες είναι «μία φορά στη ζωή». Αυτό συχνά οδηγεί σε βιαστικές και απερίσκεπτες αποφάσεις εκ μέρους των θυμάτων.

Η επίγνωση αυτών των τακτικών είναι το πρώτο βήμα για την προστασία από την απάτη μέσω ψεύτικων επενδύσεων. Είναι σημαντικό οι επενδυτές να ελέγχουν πάντα την πηγή οποιασδήποτε επενδυτικής προσφοράς και να είναι σκεπτικοί για τις υποσχέσεις υψηλών κερδών με χαμηλό κίνδυνο. Είναι επίσης σημαντικό να συμβουλευτείτε αξιόπιστους χρηματοοικονομικούς συμβούλους και να κάνετε διεξοδικούς ελέγχους πριν δεσμευτείτε σε οποιοδήποτε είδος επένδυσης.

Παραδείγματα απάτης

Η απάτη ψευδών επενδύσεων αντιπροσωπεύει μια τεράστια και διαφοροποιημένη περιοχή στον κόσμο του οικονομικού εγκλήματος, η καθεμία με τις δικές της ξεχωριστές ιδιαιτερότητες και μηχανισμούς. Τα συστήματα αυτά είναι συχνά έξυπνα σχεδιασμένα, με κύριο στόχο την εκμετάλλευση της εμπιστοσύνης και της έλλειψης πληροφόρησης των δυνητικών θυμάτων. Οι εγκληματίες που ενορχηστρώνουν τέτοιες απάτες είναι συχνά πολύ ενημερωμένοι σχετικά με την ανθρώπινη ψυχολογία και τους μηχανισμούς της χρηματοπιστωτικής αγοράς, χρησιμοποιώντας αυτή τη γνώση για να καλύψουν τις παράνομες δραστηριότητές τους.

Ένα βασικό στοιχείο για την επιτυχία αυτών των συστημάτων είναι η παρουσίασή τους ως νόμιμων και εξαιρετικά κερδοφόρων επενδυτικών ευκαιριών. Συχνά συσκευάζονται και προωθούνται με παραπλανητικό τρόπο, χρησιμοποιώντας γλώσσα και γραφικά του χρηματοπιστωτικού κλάδου για να φαίνονται αυθεντικά. Οι εγκληματίες μπορούν να χρησιμοποιήσουν διάφορα κανάλια, από το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης έως τα παραδοσιακά δίκτυα πωλήσεων, για να προσεγγίσουν ένα ευρύτερο κοινό.

Συστήματα Ponzi:

- Αυτά τα σχήματα πήραν το όνομά τους από τον Charles Ponzi, ο οποίος χρησιμοποίησε αυτή τη μέθοδο στη δεκαετία του 1920. Η ουσία ενός σχήματος Ponzi είναι να πληρώσει τα κέρδη των υφιστάμενων επενδυτών από κεφάλαια που εισάγονται από νέους επενδυτές, αντί να παράγει πραγματικά κέρδη.
- Τα συστήματα Ponzi συχνά ξεκινούν πληρώνοντας υψηλά κέρδη για να προσελκύσουν ακόμη περισσότερους επενδυτές. Αλλά καθώς ο αριθμός των νέων επενδυτών μειώνεται, τα κεφάλαια για την πληρωμή κερδών εξαντλούνται, γεγονός που αναπόφευκτα οδηγεί στην κατάρρευση του συστήματος.
- Ένα διαβόητο παράδειγμα είναι το σχέδιο του Bernie Madoff, το οποίο ήταν η μεγαλύτερη απάτη αυτού του τύπου στην ιστορία.

Επενδύσεις σε ανύπαρκτα αγαθά:

- Αυτά τα συστήματα περιλαμβάνουν υποσχέσεις για επενδύσεις σε έργα ή περιουσιακά στοιχεία που είναι είτε εντελώς πλασματικά είτε υπερβολικά υπερβολικά στην αξία τους.
- Παραδείγματα μπορεί να περιλαμβάνουν επενδύσεις σε αναξιοποίητα ορυχεία χρυσού, σπάνιες εκτάσεις ή ρηξικέλευθες τεχνολογίες. Οι εγκληματίες δημιουργούν συναρπαστικές ιστορίες, με ψευδή έγγραφα και μαρτυρίες για να φαίνονται νόμιμες.
- Τα θύματα δελεάζονται με την προοπτική μεγάλων και γρήγορων κερδών, αλλά στην πραγματικότητα, αυτά τα περιουσιακά στοιχεία ή έργα δεν υπάρχουν ή είναι εντελώς μη βιώσιμα.

Ψεύτικες προσφορές μετοχών:

- Αυτή η μέθοδος περιλαμβάνει την πώληση μετοχών για εταιρείες που δεν υπάρχουν ή που είναι υπερτιμημένες. Οι εγκληματίες μπορούν να δημιουργήσουν ψεύτικους ιστότοπους και υλικό μάρκετινγκ για να πείσουν τους επενδυτές για τις δυνατότητες της «εταιρείας».

- Χρησιμοποιούνται συχνά σε αυτό που ονομάζεται "pump and dump", όπου η αξία των μετοχών διογκώνεται τεχνητά, μετά την οποία οι εγκληματίες τις πωλούν γρήγορα πριν καταρρεύσουν.
- Τα θύματα βρίσκονται να κατέχουν μετοχές που είναι ουσιαστικά άχρηστες.

Επένδυση σε κρυπτονομίσματα:

- Με την αυξανόμενη δημοτικότητα των κρυπτονομισμάτων, έχουν επίσης αναπτυχθεί πολλά ψεύτικα επενδυτικά σχήματα που βασίζονται σε κρυπτονομίσματα.
- Αυτά τα συστήματα μπορεί να περιλαμβάνουν νέα, άγνωστα κρυπτονομίσματα που διαφημίζονται ως το επόμενο Bitcoin ή επενδυτικές πλατφόρμες που υπόσχονται υψηλά κέρδη από τις συναλλαγές κρυπτονομισμάτων.
- Πολλά από αυτά τα συστήματα καταρρέουν μετά την άντληση επαρκούς ποσού κεφαλαίων, αφήνοντας τους επενδυτές με σημαντικές απώλειες.

Επενδύσεις που πραγματοποιήθηκαν σε ψεύτικες πλατφόρμες:

- Το θύμα πείθεται να χρησιμοποιήσει μια ψεύτικη επενδυτική πλατφόρμα, η οποία διευθύνεται από εγκληματίες.
- Η πλατφόρμα είναι ένας τέλειος κλώνος επενδυτικών πλατφορμών, προσφέροντας στους χρήστες τις αξίες των μετοχών, το ποσό που κερδίζουν, την ευκαιρία να αγοράσουν και άλλες μετοχές, αλλά αυτό που δεν γνωρίζει το θύμα είναι ότι όλες οι αξίες αλλάζουν από τον εγκληματία επειδή η πλατφόρμα δεν επικοινωνεί με επενδυτικές υποδομές.
- Μεγάλα κέρδη επιτυγχάνονται μόνο ως μέλος VIP και αυτή η κατάσταση κερδίζεται μέσω σοβαρών επενδύσεων, αλλά στην πραγματικότητα είναι ένας τρόπος να πειστεί ο χρήστης να "επενδύσει" περισσότερα χρήματα.

Η αναγνώριση αυτών των τύπων ψεύτικων συστημάτων είναι ζωτικής σημασίας για κάθε επενδυτή. Είναι ζωτικής σημασίας να διεξάγετε διεξοδική έρευνα, να συμβουλευτείτε αξιόπιστους οικονομικούς εμπειρογνώμονες και να αποφύγετε οποιαδήποτε επένδυση που φαίνεται πολύ καλή για να είναι αληθινή. Η επαγρύπνηση και η εκπαίδευση είναι τα καλύτερα όπλα κατά αυτών των μορφών οικονομικής απάτης.

3. Εφαρμογές που χρησιμοποιούνται και πρόσβαση σε τραπεζικούς λογαριασμούς

Επικίνδυνες τακτικές εγκατάστασης εφαρμογών

Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν μια ποικιλία εξελιγμένων μεθόδων για να εξαπατήσουν τους χρήστες να εγκαταστήσουν επικίνδυνες εφαρμογές που τους επιτρέπουν την πρόσβαση σε τραπεζικούς λογαριασμούς και άλλες ευαίσθητες πληροφορίες. Η κατανόηση αυτών των τακτικών είναι ζωτικής σημασίας για την αναγνώριση και την πρόληψη απειλών για την προσωπική και οικονομική ασφάλεια.

Μηνύματα ηλεκτρονικού ψαρέματος (phishing) και μηνύματα ηλεκτρονικού ταχυδρομείου:

- Μία από τις πιο συνηθισμένες μεθόδους είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων που φαίνεται να προέρχονται από χρηματοπιστωτικά ιδρύματα ή άλλες αξιόπιστες οντότητες. Αυτά τα μηνύματα ενδέχεται να ζητήσουν από τους χρήστες να κατεβάσουν μια εφαρμογή για "ενημερώσεις ασφαλείας" ή να "ελέγξουν για πρόσφατες συναλλαγές".
- Τα μηνύματα ηλεκτρονικού ψαρέματος (phishing) είναι συχνά πολύ πειστικά και μπορεί να περιλαμβάνουν λογότυπα και σχέδια που μιμούνται εκείνα των νόμιμων ιδρυμάτων.

<u>Παραπλανητικές διαφημίσεις σε διαδικτυακές πλατφόρμες:</u>

- Οι διαφημίσεις στο διαδίκτυο μπορούν να χρησιμοποιηθούν για την προώθηση εφαρμογών που φαίνονται νόμιμες, αλλά στην πραγματικότητα είναι εργαλεία κακόβουλου λογισμικού. Αυτές οι διαφημίσεις μπορούν να εμφανίζονται σε αξιοσέβαστους ιστότοπους, κάνοντάς τους να φαίνονται πιο πιστευτοί.
- Μερικές φορές αυτές οι διαφημίσεις μπορούν να εκμεταλλευτούν τις ευπάθειες του προγράμματος περιήγησης για να ξεκινήσουν την αυτόματη λήψη της επικίνδυνης εφαρμογής.

Πλαστογράφηση δημοφιλών εφαρμογών:

- Οι εγκληματίες μπορούν να δημιουργήσουν ψεύτικες εκδόσεις δημοφιλών εφαρμογών που, μόλις εγκατασταθούν, μπορούν να έχουν πρόσβαση σε εμπιστευτικές πληροφορίες. Αυτές οι εφαρμογές κλωνοποίησης μπορούν να βρεθούν σε ανεπίσημα καταστήματα εφαρμογών ή ακόμα και σε ορισμένες περιπτώσεις σε επίσημες πλατφόρμες.
- Οι χρήστες μπορούν να δελεαστούν να κατεβάσουν αυτές τις εφαρμογές με υποσχέσεις πρόσθετων λειτουργιών ή αντιγράφοντας ορισμένες πτυχές των αρχικών εφαρμογών.

Εκμετάλλευση παραβιασμένων ή ψεύτικων ιστοσελίδων

- Οι εγκληματίες μπορούν να χρησιμοποιούν παραβιασμένες ή ψεύτικες ιστοσελίδες, των οποίων η εικόνα και η λειτουργικότητα είναι παρόμοια με εκείνη των νόμιμων επενδυτικών πλατφορμών, παραπλανώντας τα θύματα.
- Οι χρήστες που κατευθύνονται σε αυτές τις ψεύτικες πλατφόρμες θα ζήσουν την εμπειρία ενός επενδυτή, θα δουν

<u>Εκμετάλλευση και ανταλλαγή μηνυμάτων στα μέσα κοινωνικής δικτύωσης:</u>

- Οι εγκληματίες μπορούν να χρησιμοποιήσουν παραβιασμένους ή ψεύτικους λογαριασμούς κοινωνικών μέσων για να στείλουν συνδέσμους λήψης σε κακόβουλες εφαρμογές. Τα μηνύματα μπορούν να προέρχονται από φίλους ή γνωστούς του θύματος, αυξάνοντας τις πιθανότητες να εμπιστευτούν και να κατεβάσουν την εφαρμογή.

Κωδικός QR και άμεσοι σύνδεσμοι:

- Οι κωδικοί QR ή οι άμεσοι σύνδεσμοι που οδηγούν σε λήψεις εφαρμογών μπορούν να τοποθετηθούν σε δημόσιους χώρους ή σε διαφημιστικό υλικό. Μόλις σαρωθούν ή προσπελαστούν, μπορούν να ξεκινήσουν τη λήψη μιας επικίνδυνης εφαρμογής χωρίς τη γνώση του χρήστη.

Γνωρίζοντας τις τακτικές που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για τη διάδοση επικίνδυνων εφαρμογών, οι χρήστες μπορούν να λάβουν πιο αποτελεσματικές προφυλάξεις για την προστασία των προσωπικών και οικονομικών τους δεδομένων. Η κατανόηση των κινδύνων που σχετίζονται με τη λήψη και την εγκατάσταση μη εξουσιοδοτημένων εφαρμογών είναι ένα κρίσιμο πρώτο βήμα για τη διασφάλιση της ασφάλειας στο διαδίκτυο.

Κίνδυνοι που σχετίζονται με εφαρμογές που χρησιμοποιούνται

Οι κίνδυνοι που συνδέονται με τις εφαρμογές που χρησιμοποιούνται από εγκληματίες στον κυβερνοχώρο είναι ποικίλοι και μπορούν να έχουν σοβαρές συνέπειες τόσο για την ατομική ασφάλεια όσο και για την ακεραιότητα των οικονομικών δεδομένων των χρηστών. Αυτές οι κακόβουλες εφαρμογές έχουν σχεδιαστεί για να κλέβουν πληροφορίες, να θέτουν σε κίνδυνο συσκευές και να διευκολύνουν τη μη εξουσιοδοτημένη πρόσβαση σε χρηματοοικονομικά περιουσιακά στοιχεία και προσωπικούς λογαριασμούς.

Κλοπή ταυτότητας:
Οι επικίνδυνες εφαρμογές μπορούν να συλλέγουν προσωπικές πληροφορίες, όπως ονόματα, διευθύνσεις, ημερομηνίες γέννησης, ακόμη και αριθμούς κοινωνικής ασφάλισης. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για τη διάπραξη κλοπής ταυτότητας, επιτρέποντας στους εγκληματίες να έχουν πρόσβαση σε τραπεζικούς λογαριασμούς, να ανοίγουν νέα δάνεια ή να διαπράττουν άλλα εγκλήματα με την ταυτότητα του θύματος.

Πρόσβαση σε οικονομικές πληροφορίες:
Πολλές από αυτές τις εφαρμογές στοχεύουν άμεσα στην κλοπή οικονομικών πληροφοριών, όπως αριθμούς πιστωτικών καρτών, διαπιστευτήρια τραπεζικού λογαριασμού στο διαδίκτυο και άλλα οικονομικά στοιχεία. Η πρόσβαση σε αυτές τις πληροφορίες μπορεί να οδηγήσει σε κλοπή κεφαλαίων ή μη εξουσιοδοτημένες συναλλαγές.

Κατάργηση/Επηρεασμός πολλαπλού ελέγχου ταυτότητας (2FA / MFA)
Η υποκλοπή ή ο χειρισμός διπλού/πολλαπλού ελέγχου ταυτότητας τραπεζικών εφαρμογών θα επιτρέψει στους εγκληματίες του κυβερνοχώρου να επαληθεύουν συνεχώς την ταυτότητά τους σε τραπεζικές εφαρμογές, να τροποποιούν δεδομένα πρόσβασης και να συναλλάσσονται σιωπηρά απευθείας από την εφαρμογή, χωρίς το θύμα να βλέπει τις δραστηριότητές τους.

Κακόβουλο λογισμικό και ransomware:
Ορισμένες εφαρμογές μπορούν να εγκαταστήσουν κακόβουλο λογισμικό ή ransomware στη συσκευή του θύματος. Το κακόβουλο λογισμικό μπορεί να παρακολουθεί τις

δραστηριότητες των χρηστών, να υποκλέπτει δεδομένα ή να βλάπτει το σύστημα. Το ransomware αποκλείει την πρόσβαση σε δεδομένα στη συσκευή σας, απαιτώντας λύτρα για να την ξεκλειδώσετε.

Διακυβεύεται η ασφάλεια της συσκευής:
Η εγκατάσταση επικίνδυνων εφαρμογών μπορεί να αποδυναμώσει τη συνολική ασφάλεια της συσκευής σας, καθιστώντας την ευάλωτη σε πρόσθετες επιθέσεις. Αυτό μπορεί να περιλαμβάνει το άνοιγμα θυρών δικτύου, την απενεργοποίηση της προστασίας από ιούς ή τη δημιουργία κενών για την πρόσβαση άλλων εγκληματιών στη συσκευή σας.

Κατασκοπεία και παρακολούθηση:
Ορισμένες εφαρμογές μπορούν να χρησιμοποιηθούν για την κατασκοπεία των δραστηριοτήτων των χρηστών, συμπεριλαμβανομένης της πρόσβασης στην κάμερα και το μικρόφωνο της συσκευής. Αυτό μπορεί να οδηγήσει σε σοβαρές παραβιάσεις της ιδιωτικής ζωής και στη συλλογή ευαίσθητων πληροφοριών.

Phishing και κοινωνική μηχανική:
Οι εφαρμογές μπορούν επίσης να χρησιμοποιηθούν για την εκτέλεση καμπανιών ηλεκτρονικού ψαρέματος (phishing), στέλνοντας ψεύτικα μηνύματα που φαίνεται να προέρχονται από αξιόπιστες πηγές για την απόκτηση ευαίσθητων πληροφοριών.

Βλάβη φήμης:
Σε περιπτώσεις όπου οι εγκληματίες αποκτούν πρόσβαση στους λογαριασμούς κοινωνικών μέσων του θύματος, ενδέχεται να στείλουν μηνύματα ή αναρτήσεις που ενδέχεται να βλάψουν τη φήμη αυτού του ατόμου.

4. Απεικόνιση του συστήματος απάτης

Η πολυπλοκότητα της διαδικασίας απάτης

Η διαδικασία απάτης είναι αρκετά περίπλοκη και έχει διάφορες παραλλαγές ανάπτυξης, ανάλογα με το επίπεδο κατάρτισης του χρήστη (δυνητικού θύματος) από τεχνική άποψη και τη δύναμη πειθούς του δράστη έναντι του ατόμου που έχει ήδη φτάσει στη φάση επικοινωνίας μαζί του.

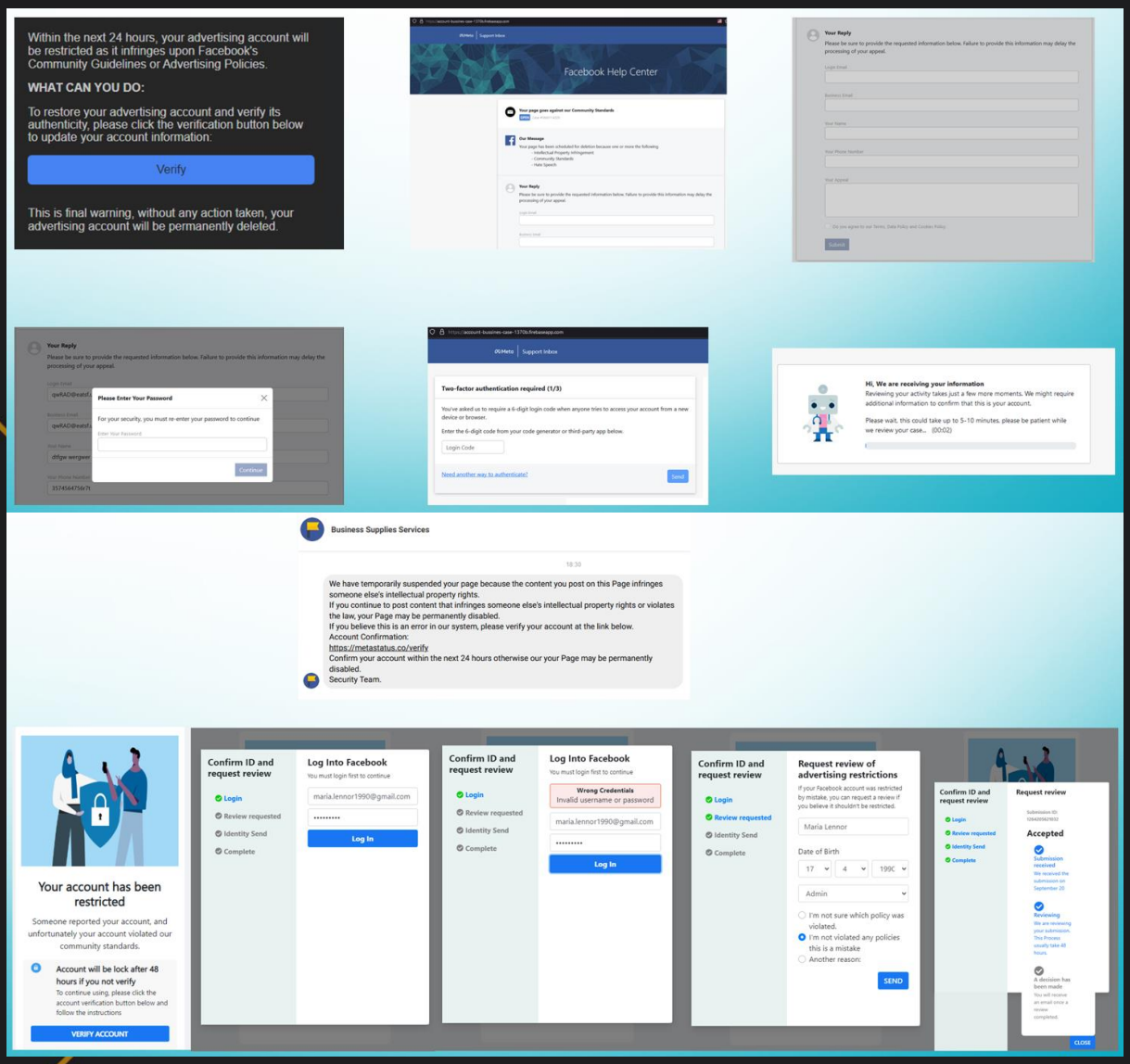
Η αρχική επίθεση – απόκτηση των απαραίτητων πόρων

Μια πρώτη σημαντική πτυχή στη διαδικασία απάτης είναι η επαφή με πιθανά θύματα, η οποία μπορεί να γίνει με άμεσο τρόπο, μέσω στοχευμένης προσέγγισης ή με έμμεσο τρόπο με την τοποθέτηση ψευδών πληροφοριών στο διαδικτυακό περιβάλλον, μέσω μηνυμάτων, αναρτήσεων, σχολίων ή / και διαφημίσεων που προωθούν το σενάριο απάτης.

a. Νέοι λογαριασμοί: Λογαριασμοί κοινωνικών μέσων ή άλλες πλατφόρμες που έχουν δημιουργηθεί ειδικά για την προώθηση πληροφοριών στο διαδίκτυο. Χαμηλή αξιοπιστία στην άμεση προσέγγιση, αλλά με αντίκτυπο εάν προστεθεί σε παραβιασμένες σελίδες κοινωνικών μέσων.

b. Παραβιασμένοι λογαριασμοί: Λογαριασμοί που αποκτώνται με την αγορά τους ή με άλλες μεθόδους, όπως κακόβουλο λογισμικό ή ηλεκτρονικό ψάρεμα (phishing).

Παράδειγμα κυβερνοεπίθεσης ηλεκτρονικού ψαρέματος (phishing), η οποία πραγματοποιήθηκε μέσω μηνυμάτων ή/και με προσθήκη ετικέτας στο άτομο ή τη σελίδα που κατείχε. Αυτά τα μηνύματα ανακοίνωσαν την παραβίαση των κανόνων της πλατφόρμας και ζήτησαν από τους ιδιοκτήτες να επιβεβαιώσουν την ταυτότητά τους, ώστε να μην χάσουν την πρόσβαση.



Η πρόσβαση και οι προσωπικές πληροφορίες που προστέθηκαν σε ψεύτικες σελίδες έδωσαν στους επιτιθέμενους πρόσβαση στους λογαριασμούς των θυμάτων, με το επόμενο βήμα να είναι να εμποδίσουν τους νόμιμους κατόχους να έχουν πρόσβαση σε παραβιασμένους λογαριασμούς και σελίδες. Για να διευκολύνουν τη δουλειά τους, οι δημιουργοί ψεύτικων σελίδων πρόσθεσαν επίσης τη δυνατότητα για το θύμα να δηλώσει εάν είναι διαχειριστής σελίδας.

Μια ενιαία καμπάνια αυτού του τύπου συγκέντρωσε σε λίγες μέρες 100.000 λογαριασμούς χρηστών του Facebook και αρχικά διαπιστώθηκε ότι το 10% από αυτούς ανήκουν σε θύματα

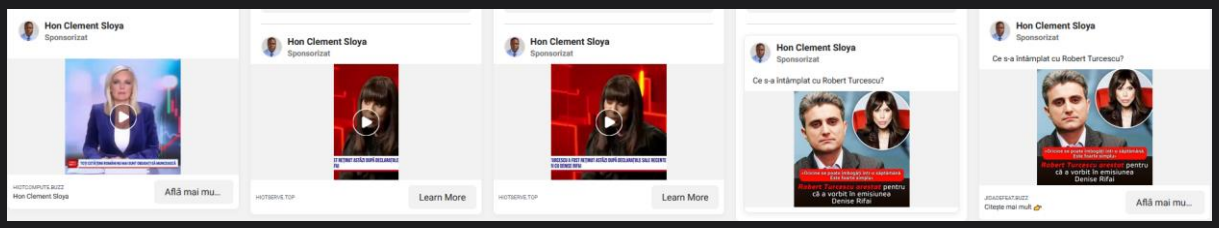
στη Ρουμανία, επειδή η ταξινόμησή τους έγινε με τον εντοπισμό γραμμών κειμένου που περιέχουν τοπικούς τομείς ".ro" και την αυτόματη ταξινόμηση που ορίζεται από τους επιτιθέμενους "| EN". Αργότερα, μετά από λεπτομερέστερη ανάλυση των δεδομένων που συλλέχθηκαν από εγκληματίες, διαπιστώθηκε ότι πολλά θύματα δεν πληρούσαν τα αρχικά κριτήρια ταξινόμησης, αλλά το όνομα και το επώνυμό τους είναι ρουμανικά. Αυτό άλλαξε το ποσοστό σε πάνω από 45% εις βάρος των Ρουμάνων χρηστών, η επίθεση στόχευε σαφώς ρουμανόφωνους, ανεξάρτητα από την τρέχουσα τοποθεσία τους.

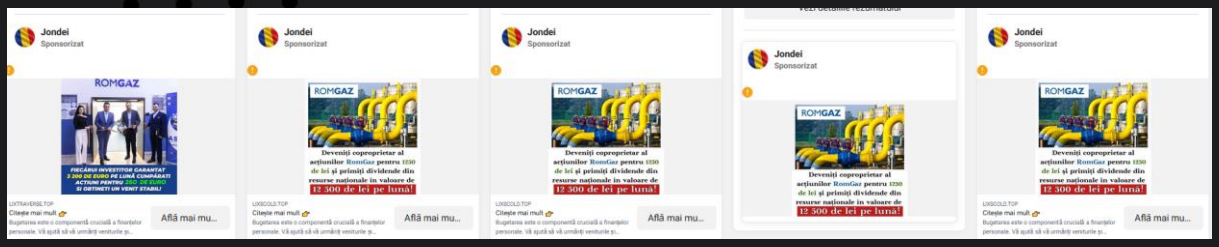
Εκμετάλλευση παραβιασμένων λογαριασμών/σελίδων – Στόχευση θυμάτων

Όταν πρόκειται για τον επιτιθέμενο, μπορεί να έχει διάφορους ρόλους στη διεξαγωγή της αρχικής επίθεσης ή μόνο έναν:

- Ο ρόλος του κυβερνοεγκληματία που ξεκινά εκστρατείες ηλεκτρονικού ψαρέματος (phishing) ή κακόβουλου λογισμικού για να αποκτήσει πρόσβαση σε δεδομένα λογαριασμών κοινωνικών μέσων,
- Ο ρόλος του δράστη που έλαβε/αγόρασε δεδομένα πρόσβασης και τα εκμεταλλεύεται ξεκινώντας το επόμενο στάδιο απάτης.

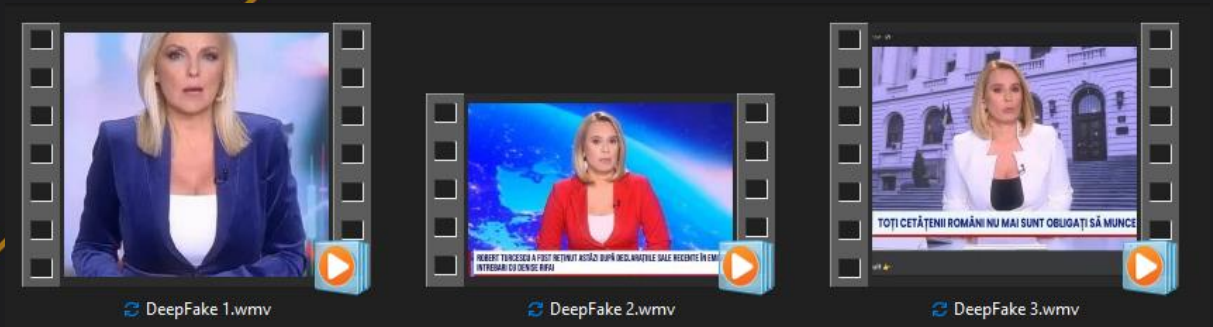
Το μεγαλύτερο συμφέρον των εισβολέων είναι να θέσουν σε κίνδυνο λογαριασμούς που διαχειρίζονται/δημιουργούν διαφημίσεις. Αυτοί οι λογαριασμοί χρησιμοποιούνται για τη δημιουργία διαφημίσεων που προωθούν την οικονομική απάτη, ενώ δημιουργούν υψηλό κόστος για παραβιασμένους και εκμεταλλευόμενους λογαριασμούς. Δαπάνες που βαρύνουν τους κατόχους τραπεζικών καρτών που έχουν εισαχθεί σε πλατφόρμες δημιουργίας διαφημίσεων.





Ο σκοπός της εκμετάλλευσης λογαριασμών είναι να προωθήσει την απάτη και να κατευθύνει έμμεσα τα πιθανά θύματα σε ψεύτικες σελίδες που χρησιμοποιούνται στη διαδικασία απάτης. Τα στάδια της διεξαγωγής αυτής της διαδικασίας φαίνονται στην εικόνα.

Και με ασυνήθιστα υψηλή συχνότητα, χρησιμοποιείται η κλοπή της οπτικής ταυτότητας ανθρώπων με επιρροή και η δημιουργία ψεύτικων ή Deep Fake ακολουθιών βίντεο (ψεύτικα βίντεο που παράγονται από την Τεχνητή Νοημοσύνη μέσω των οποίων κλωνοποιείται η εικόνα και η φωνή ενός ατόμου)

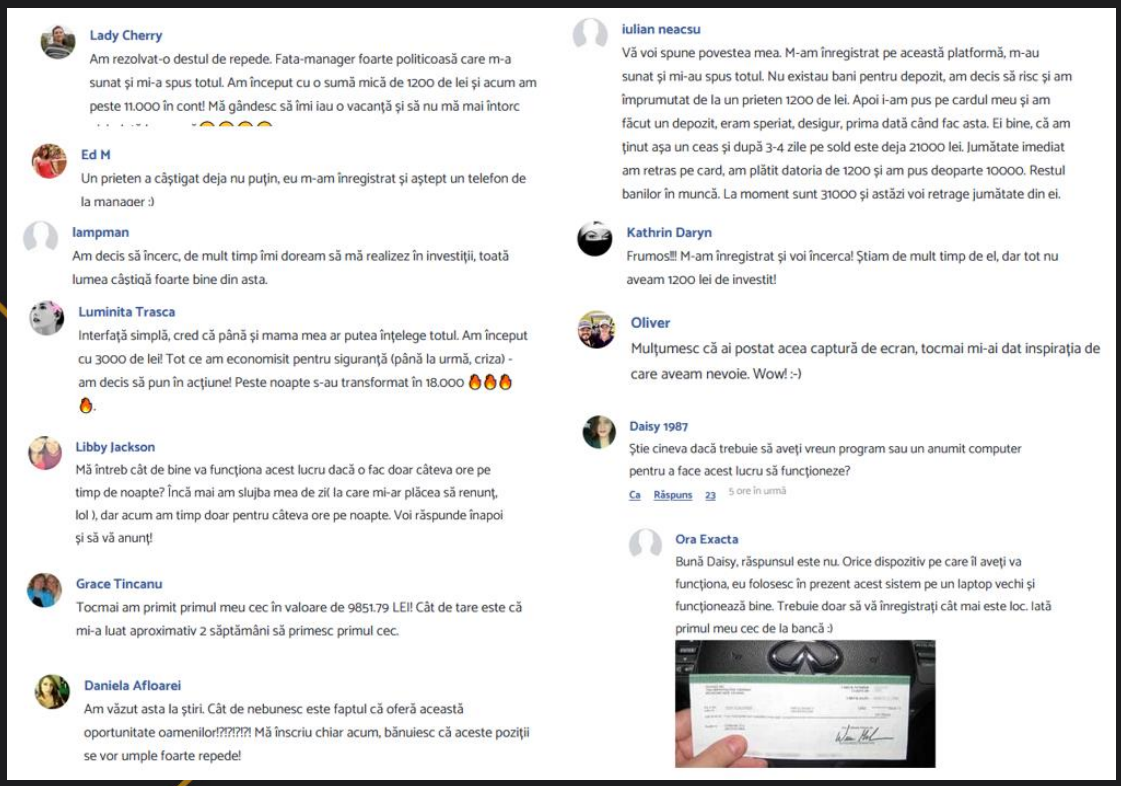


Οι απρόσεκτοι ή αμόρφωτοι χρήστες του κυβερνοχώρου θα εισέλθουν στα σενάρια που δημιουργούνται από τους επιτιθέμενους και θα παίξουν το ρόλο του θύματος, καθώς φτάνουν σε αυτή τη θέση αποδεχόμενοι οπτική χειραγώγηση. Γενικά, η χειραγώγηση γίνεται με την αποστολή πληροφοριών/προειδοποιητικών μηνυμάτων και αναφέρεται ένα προσωρινό όριο, το οποίο έχει το ρόλο της απομάκρυνσης του χρήστη από την κατάσταση άνεσής του, γεγονός που θα τον κάνει να μην δίνει προσοχή στις λεπτομέρειες.

Ο χρήστης που έφτασε στην ψεύτικη σελίδα χαιρετίζεται από μια χιονοστιβάδα εικόνων και κειμένων που υποστηρίζουν το σενάριο απάτης, αλλά περιέχουν επίσης ψευδείς δηλώσεις ατόμων που ισχυρίζονται ότι είναι ήδη μέρος αυτής της επιχείρησης, αγόρασαν το προϊόν ή επένδυσαν σε μετοχές και τα αποτελέσματα είναι αυτά που περιγράφονται από τους διαχειριστές των ψεύτικων σελίδων.

Η κοινωνική μηχανική έχει να διαδραματίσει σημαντικό ρόλο.

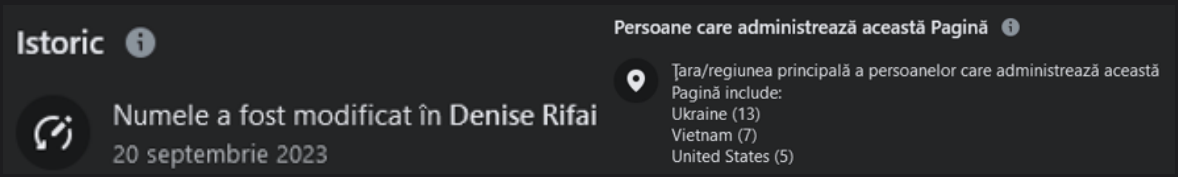
Τα ψεύτικα σχόλια περιλαμβάνουν μια πληθώρα καταστάσεων για να καλύψουν μια μεγάλη κλίμακα χρηστών τεχνολογίας που επιθυμούν να κερδίσουν χρήματα ή σχόλια προσαρμοσμένα στον απώτερο στόχο της απάτης / απάτης.



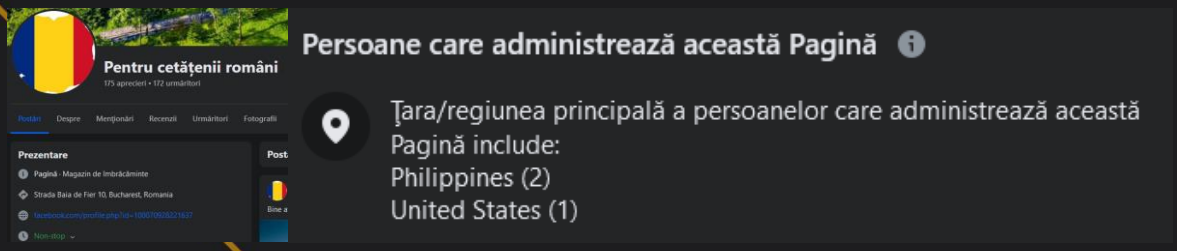
- *Τεχνική βοήθεια για όσους δεν είναι καλοί* σε αυτό, αλλά θα ήθελαν,
- *Κέρδισε έναν "φίλο"* - Έτσι είναι κάτι δοκιμασμένο,
- *Εύκολη στη χρήση εφαρμογή "που ακόμη και η μαμά θα μπορούσε ..."* - Συμπεριλάβετε ανόητους και ηλικιωμένους,
- *Παραιτηθείτε από τη δουλειά σας για υψηλά κέρδη* - Αν αυτός ο τύπος μπορεί, ας το δοκιμάσουμε.
- *"Μόλις πήρα την πρώτη μου επιταγή..."* - "Εγγύηση" κερδών,
- *"Το είδα στις ειδήσεις"* - Είναι κάτι που λέγεται στην τηλεόραση, οπότε είναι καλό...
- *"Αυτές οι θέσεις θα γεμίσουν γρήγορα..."* - Γρήγορα που ίσως δεν παίρνουμε όλοι πια.
- *«Δεν υπήρχαν χρήματα... Δανείστηκα»* – Πείθοντας όσους δεν έχουν χρήματα, αλλά μπορούν να δανειστούν.

- *«Έκανα μια κατάθεση, φοβήθηκα, ήταν η πρώτη φορά...»* – Λεπτή εξάλειψη των αμφιβολιών και της πεποίθησης να προσπαθήσω.
- ..... κλπ.

Οι σελίδες που δημιουργούν δόλιες διαφημίσεις υφίστανται σημαντικές αλλαγές εικόνας και διαχείρισης.



Παράδειγμα καμπάνιας ηλεκτρονικού ψαρέματος (phishing) σε χρήστες στη Ρουμανία. Κατά τη διάρκεια της περιόδου ανάλυσης, ο λογαριασμός είχε δημιουργήσει 420 διαφημίσεις με την εκστρατεία απάτης και σε μια τρέχουσα επαλήθευση, ο λογαριασμός υποδεικνύει έναν αριθμό 510 διαφημίσεων που δημιουργήθηκαν, η τελευταία από τις οποίες προβλήθηκε στις 26 Οκτωβρίου 2023.



Τρέχουσα κατάσταση σελίδας: Σε σύνδεση, αλλά με διαφορετικό όνομα...

... άλλη χώρα, άλλοι στόχοι απάτης.

Το ενδιαφέρον των εγκλημάτων και ο σκοπός αυτών που αναφέρονται είναι να πείσουν τους χρήστες να έχουν πρόσβαση σε ψεύτικες σελίδες και να συμπληρώσουν μια φόρμα με στοιχεία επικοινωνίας, ώστε ο υπεύθυνος της πλατφόρμας να μπορεί να έρθει σε επαφή μαζί τους.

Ή, ανάλογα με την περίπτωση, ο σκοπός της απάτης είναι να εξαπατήσει τους ανθρώπους να αγοράσουν ένα προϊόν ή μια υπηρεσία που προσφέρεται από την ψεύτικη σελίδα!

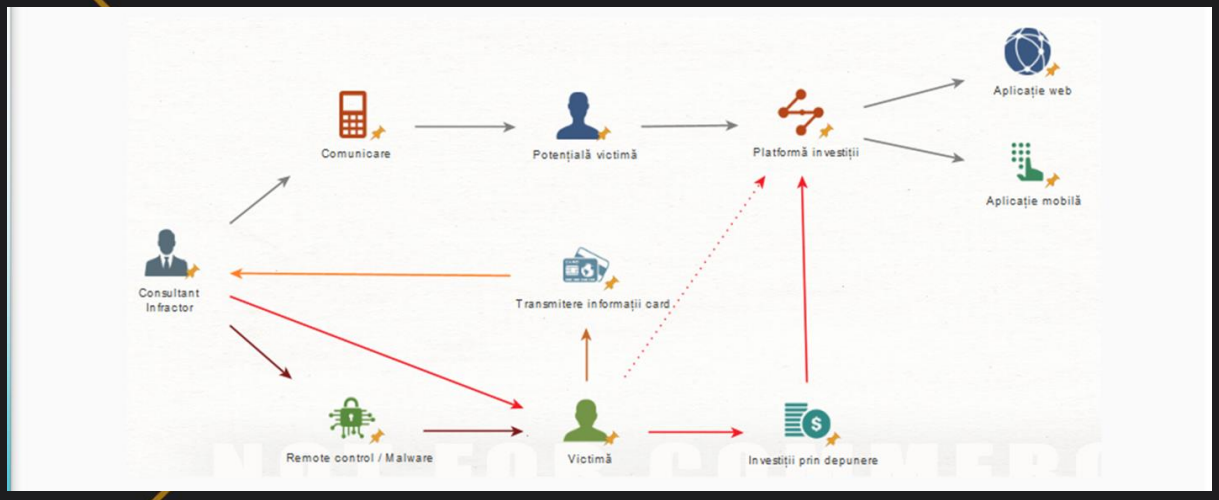
Ανάλυση των σταδίων οικονομικής απάτης

Τα στοιχεία επικοινωνίας που αποκτούν οι εγκληματίες είναι ένα σημαντικό βήμα στη διαδικασία απάτης, καθώς τα άτομα που επισκέφτηκαν την ψεύτικη σελίδα εγγράφηκαν στη λίστα πιθανών θυμάτων.

Σε αυτό το στάδιο, ο σημαντικότερος ρόλος διαδραματίζει ο Σύμβουλος, ο εγκληματίας που έρχεται σε επαφή με το πιθανό θύμα, διότι, μέσω της κοινωνικής μηχανικής, θα κάνει ό, τι είναι δυνατόν για τον συνομιλητή του να πιστέψει ολόκληρο το σενάριο γύρω από την απάτη και να τον πείσει ότι είναι 100% νικητής σε αυτή την επιχείρηση.

Διατηρώντας ως κύριο θέμα την οικονομική απάτη μέσω επενδύσεων σε κρυπτονομίσματα ή μετοχών επιτυχημένων εταιρειών, θα πρέπει να γίνει κατανοητό ότι ο εισβολέας θα έρθει σε επαφή με χρήστες με διαφορετικά επίπεδα εκπαίδευσης, τεχνικές δεξιότητες και ηλικία. Οι έρευνες διαπίστωσαν ότι οι οικονομικές απώλειες προέκυψαν μέσω άμεσων επενδύσεων από χρήστες, αποστολής κεφαλαίων σε εγκληματίες, χρήσης ψεύτικων εφαρμογών και χρήσης εφαρμογών απομακρυσμένου ελέγχου, δίνοντας στους εγκληματίες πρόσβαση στις συσκευές των χρηστών για να τους βοηθήσουν να δημιουργήσουν λογαριασμούς σε ψεύτικες πλατφόρμες και ακόμη και χρησιμοποιώντας τις τραπεζικές εφαρμογές τους.

Η ροή των δραστηριοτήτων που διεξάγονται μπορεί να γίνει κατανοητή από την παρακάτω εικόνα, αλλά ταυτόχρονα μπορεί κανείς να παρατηρήσει την προσαρμοστικότητα των δραστών στο επίπεδο κατάρτισης των θυμάτων, μερικές φορές μέρος των στόχων που πρέπει να εξαλειφθούν, επειδή φτάνουν τα χρήματα χωρίς να απαιτούν μεγάλη προσπάθεια.



Ολοκληρώνοντας αναλύοντας τη διαδικασία απάτης, έχουμε μια σαφή εικόνα των ρόλων των εγκληματιών, των χρηστών και των οικονομικών απωλειών.

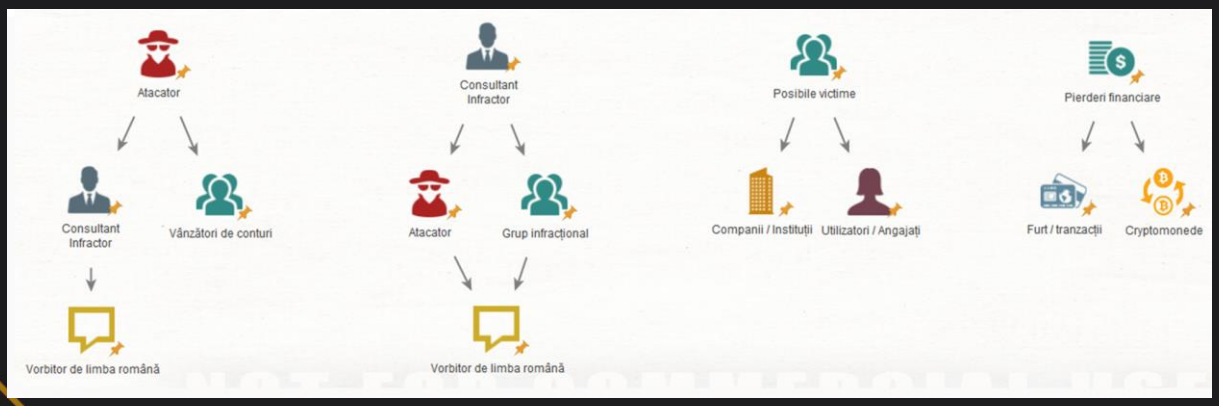
Ο αρχικός εισβολέας μπορεί να είναι μόνο το άτομο που ξεκινά τις καμπάνιες ηλεκτρονικού ψαρέματος / κακόβουλου λογισμικού, για να αποκτήσει δεδομένα πρόσβασης και να τα πουλήσει σε εγκληματίες που θα ασχοληθούν με την απάτη, μπορεί να είναι μέρος της ομάδας απάτης ή ένα και το ίδιο άτομο με τον σύμβουλο που ολοκληρώνει τη διαδικασία απάτης.

Ο σύμβουλος μπορεί να είναι, όπως αναφέρθηκε, ο ίδιος ο αρχικός επιτιθέμενος ή είναι μέρος μιας εγκληματικής ομάδας, στην οποία ο καθένας έχει το ρόλο του. Σύμφωνα με τις

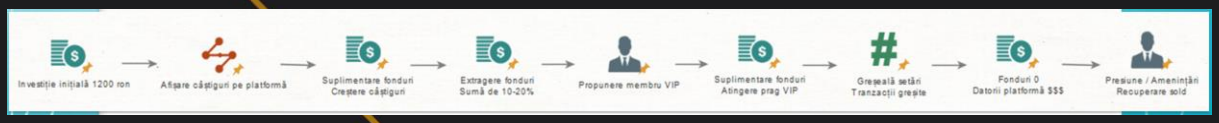
δηλώσεις των θυμάτων, οι δράστες είναι ρουμανόφωνοι, συχνά με συγκεκριμένη ρωσική προφορά.

Πιθανά θύματα είναι εταιρείες/ιδρύματα των οποίων οι λογαριασμοί έχουν παραβιαστεί και αξιοποιηθεί για τη δημιουργία διαφημίσεων και οι χρήστες που εμπλέκονται σε κάθε στάδιο του σεναρίου απάτης.

Τα θύματα απάτης (ψεύτικες επενδύσεις) είναι χρήστες πρόθυμοι για γρήγορα κέρδη, αλλά στερούνται ψηφιακής εκπαίδευσης, εκπαίδευσης στον κυβερνοχώρο και εύκολα χειραγωγούμενων ανθρώπων.



Οι μεγάλες οικονομικές απώλειες οφείλονται στη χειραγώγηση του θύματος στην επενδυτική διαδικασία, στους εγκληματίες που εφαρμόζουν τεχνικές για να κερδίσουν την εμπιστοσύνη του θύματος, αλλά μπορεί να φτάσει μέχρι την επιβολή χρεών στην επενδυτική πλατφόρμα και ακόμη και απειλές για την ανάκτηση πλασματικών εκκρεμών υπολοίπων.



5. Πρόληψη και προστασία των χρηστών

Προειδοποιητικά σημάδια πιθανής απάτης

Τα προειδοποιητικά σημάδια πιθανής οικονομικής απάτης είναι ζωτικής σημασίας για την αναγνώριση και την πρόληψη της πτώσης στις παγίδες των εγκληματιών. Κάθε ένα από αυτά τα σημάδια υποδεικνύει πιθανούς κινδύνους και απαιτεί αυξημένη επαγρύπνηση από τους χρήστες:

a. Προσφορές με ασυνήθιστα υψηλές αποδόσεις:

Στον κόσμο των επενδύσεων, ένας γενικός εμπειρικός κανόνας είναι ότι οι υψηλές αποδόσεις συνήθως συνοδεύονται από αντίστοιχους κινδύνους. Κάθε προσφορά που υπόσχεται σημαντικά κέρδη χωρίς αντίστοιχο κίνδυνο είναι ύποπτη. Αυτές οι προσφορές μπορεί να αποτελούν μέρος ενός συστήματος Ponzi ή άλλων τύπων απάτης.

b. Πίεση για γρήγορη δράση:

Η τακτική της δημιουργίας επείγοντος χρησιμοποιείται συχνά για να αποτρέψει τους πιθανούς επενδυτές από την κριτική ανάλυση της προσφοράς. Σε αυτές τις περιπτώσεις, οι εγκληματίες μπορεί να υποστηρίξουν ότι η ευκαιρία είναι «μια φορά στη ζωή» ή ότι απαιτείται άμεση δράση για να επωφεληθούν από τις συνθήκες που προσφέρονται.

c. Αιτήματα για προσωπικές ή οικονομικές πληροφορίες:

Τα απροσδόκητα αιτήματα για ευαίσθητες πληροφορίες αποτελούν σαφή ένδειξη απάτης. Οι εγκληματίες μπορούν να χρησιμοποιήσουν αυτά τα δεδομένα για πρόσβαση σε τραπεζικούς λογαριασμούς, για κλοπή ταυτότητας ή άλλες παράνομες δραστηριότητες. Οποιοδήποτε τέτοιο αίτημα θα πρέπει να αντιμετωπίζεται με μεγάλη προσοχή.

d. Έλλειψη διαφάνειας ή ασαφής τεκμηρίωση:

Οι νόμιμες επενδυτικές προσφορές είναι συνήθως διαφανείς και συνοδεύονται από σαφή και λεπτομερή τεκμηρίωση. Η έλλειψη διαφάνειας, η διφορούμενη ή ασαφής τεκμηρίωση ή η απροθυμία απάντησης σε συγκεκριμένες ερωτήσεις είναι σημάδια ότι κάτι δεν πάει καλά.

e. Αυτόκλητη επικοινωνία:

Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, τηλεφωνικές κλήσεις ή μηνύματα που προσφέρουν επενδυτικές ευκαιρίες ή ζητούν προσωπικές πληροφορίες θα πρέπει να αντιμετωπίζονται με καχυποψία. Αυτές οι μέθοδοι χρησιμοποιούνται συχνά σε καμπάνιες ηλεκτρονικού ψαρέματος (phishing) για την απόκτηση πρόσβασης σε εμπιστευτικές πληροφορίες.

Η αναγνώριση αυτών των προειδοποιητικών ενδείξεων είναι ένα κρίσιμο βήμα για την προστασία από την οικονομική απάτη. Είναι σημαντικό για τους χρήστες να επαγρυπνούν, να κάνουν ερωτήσεις και να διεξάγουν διεξοδική έρευνα πριν λάβουν οποιεσδήποτε οικονομικές αποφάσεις. Η πρόληψη ξεκινά με την ενημέρωση και την ευαισθητοποίηση σχετικά με τους κινδύνους.

Συμβουλές πρόληψης

Για να αποφύγετε τις παγίδες της οικονομικής απάτης, είναι σημαντικό να ακολουθήσετε μια προληπτική και ενημερωμένη προσέγγιση για τη διαχείριση των οικονομικών και των προσωπικών σας πληροφοριών. Ακολουθούν ορισμένες λεπτομερείς συμβουλές πρόληψης που μπορούν να σας προστατεύσουν:

a. Διεξαγωγή διεξοδικής έρευνας:

- Επαλήθευση πηγής: Πριν επενδύσετε, βεβαιωθείτε ότι η οικονομική οντότητα και η προσφορά είναι νόμιμες. Αναζητήστε πληροφορίες σχετικά με την εταιρεία και τα προϊόντα ή τις υπηρεσίες της.

- Διαβούλευση με τις ρυθμιστικές αρχές του χρηματοπιστωτικού τομέα: Ελέγξτε αν η οντότητα είναι εγγεγραμμένη ή ρυθμίζεται από αναγνωρισμένη χρηματοπιστωτική αρχή.
- Αναζήτηση ανεξάρτητων συμβουλών: Είναι πάντα χρήσιμο να πάρετε μια δεύτερη γνώμη από έναν ανεξάρτητο οικονομικό σύμβουλο που μπορεί να αξιολογήσει αντικειμενικά την προσφορά.
- Ζητήστε συμβουλές από ειδικούς: Ζητήστε τη γνώμη ενός επαγγελματία ασφάλειας στον κυβερνοχώρο όταν υπάρχουν υποψίες σχετικά με τις ιστοσελίδες ή τις πλατφόρμες στις οποίες έχετε κατευθυνθεί.

b. Προστατέψτε τα προσωπικά σας στοιχεία:

- Επαγρύπνηση στην επικοινωνία: Να είστε εξαιρετικά προσεκτικοί όταν σας ζητούνται προσωπικά ή οικονομικά δεδομένα. Μην παρέχετε αυτές τις πληροφορίες μέσω μη ασφαλών καναλιών ή μη εξουσιοδοτημένων ατόμων.
- Προστασία δεδομένων: Χρησιμοποιήστε τεχνικές προστασίας δεδομένων, όπως κρυπτογράφηση και ασφαλή αποθήκευση, για να διατηρήσετε τις πληροφορίες σας εμπιστευτικές. Προσωπικός.

c. Χρησιμοποιήστε πρακτικές ασφάλειας στο Internet:

- Ενημέρωση λογισμικού: Βεβαιωθείτε ότι το λειτουργικό σύστημα και οι εφαρμογές σας είναι πάντα ενημερωμένα, για προστασία από ευπάθειες ασφαλείας.
- Χρήση διπλού/πολλαπλού ελέγχου ταυτότητας: Ενεργοποιεί τον έλεγχο ταυτότητας πολλών παραγόντων σε όλους τους κύριους λογαριασμούς για να προσθέσει ένα επιπλέον επίπεδο ασφάλειας.

d. Αποφύγετε τις παρορμητικές αποφάσεις:

- Ανάλυση και προβληματισμός: Αφιερώστε χρόνο για να αξιολογήσετε κάθε οικονομική ευκαιρία και να σταθμίσετε τα υπέρ και τα κατά. Μια καλά μελετημένη οικονομική απόφαση είναι πάντα ασφαλέστερη.
- Αποφύγετε την πίεση: Μην πιέζεστε να πάρετε γρήγορες αποφάσεις, ειδικά σε αγχωτικές ή πιεστικές καταστάσεις.

e. Παρακολουθήστε τους οικονομικούς λογαριασμούς σας:

- Τακτικοί έλεγχοι: Ελέγχετε τακτικά τις κινήσεις τραπεζικών λογαριασμών και τις συναλλαγές για οποιαδήποτε ύποπτη ή μη εξουσιοδοτημένη δραστηριότητα.
- Ειδοποιήσεις συναλλαγών: Ο ορισμός ειδοποιήσεων για ασυνήθιστες ή μεγάλες συναλλαγές μπορεί να είναι ένας αποτελεσματικός τρόπος γρήγορου εντοπισμού απάτης.

Εφαρμόζοντας αυτές τις πρακτικές, θα είστε σε θέση να αυξήσετε το επίπεδο προστασίας σας από πιθανή οικονομική απάτη. Η ευαισθητοποίηση και η συνεχής εκπαίδευση είναι απαραίτητες σε αυτή τη διαδικασία, καθώς οι μέθοδοι των παραβατών μπορούν να αλλάξουν και να εξελιχθούν. Έχετε πάντα το νου σας για τις τελευταίες τακτικές απάτης και

προσαρμόζετε ανάλογα τις στρατηγικές ασφαλείας σας για να διατηρήσετε τα οικονομικά σας ασφαλή.

6. Ο ρόλος των χρηματοπιστωτικών ιδρυμάτων

Μέτρα ασφάλειας και παρακολούθησης

a. Προηγμένα συστήματα ανίχνευσης απάτης:

- Αυτά τα συστήματα χρησιμοποιούν εξελιγμένους αλγόριθμους και μηχανική μάθηση για τον εντοπισμό ασυνήθιστων ή ύποπτων συναλλαγών, βοηθώντας στον έγκαιρο εντοπισμό πιθανής απάτης.
- Η ανάλυση συμπεριφοράς και η μοντελοποίηση κινδύνου χρησιμοποιούνται επίσης για την αξιολόγηση των μοτίβων συναλλαγών και τον εντοπισμό ασυνήθιστης δραστηριότητας.

b. Ασφάλεια τεχνολογικής υποδομής:

- Η διασφάλιση της υποδομής πληροφορικής περιλαμβάνει την προστασία των δεδομένων των πελατών και των τραπεζικών συστημάτων από κυβερνοεπιθέσεις χρησιμοποιώντας προηγμένες τεχνολογίες κρυπτογράφησης και ισχυρές λύσεις ασφάλειας.
- Η συνεχής ενημέρωση και συντήρηση των συστημάτων πληροφορικής είναι ζωτικής σημασίας για να παραμείνουμε μπροστά από τις ολοένα και πιο εξελιγμένες μεθόδους των εγκληματιών στον κυβερνοχώρο.

c. Έλεγχος ταυτότητας πολλαπλών παραγόντων και ασφάλεια λογαριασμού:

- Η εφαρμογή του ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) παρέχει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας κάτι περισσότερο από ένα όνομα χρήστη και έναν κωδικό πρόσβασης για πρόσβαση σε έναν λογαριασμό.
- Το MFA μπορεί να περιλαμβάνει στοιχεία όπως κωδικούς που δημιουργούνται από το τηλέφωνο, ερωτήσεις ασφαλείας ή δακτυλικά αποτυπώματα, αυξάνοντας σημαντικά την ασφάλεια των διαδικτυακών λογαριασμών.

Εκπαίδευση πελατών στον τομέα της ασφάλειας στον κυβερνοχώρο

Η εκπαίδευση των πελατών στον τομέα της ασφάλειας στον κυβερνοχώρο αποτελεί κρίσιμη πτυχή της στρατηγικής των χρηματοπιστωτικών ιδρυμάτων για την καταπολέμηση της απάτης. Με την ενημέρωση και την εκπαίδευση των πελατών, μπορούν να μειώσουν σημαντικά τον κίνδυνο να πέσουν θύματα παράνομων δραστηριοτήτων στο διαδίκτυο.

a. Προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας:

- Εκπαιδευτικό υλικό: Παροχή φυλλαδίων, οδηγών και άλλου ενημερωτικού υλικού που εξηγεί διαφορετικούς τύπους απάτης στον κυβερνοχώρο, όπως phishing, vishing, smishing και άλλες τεχνικές κοινωνικής μηχανικής.
- Πραγματικά παραδείγματα και μελέτες περιπτώσεων: Η παρουσίαση πραγματικών περιπτώσεων απάτης μπορεί να βοηθήσει τους πελάτες να κατανοήσουν καλύτερα τους κινδύνους και να αναγνωρίσουν τα προειδοποιητικά σημάδια.

b. Τακτική επικοινωνία με τους πελάτες:

- Ενημερωτικά δελτία: Περιοδική αποστολή ενημερωτικών δελτίων που περιλαμβάνουν συμβουλές ασφαλείας, προειδοποιήσεις σχετικά με νέους τύπους απάτης και συστάσεις για προστασία στο Internet.
- Κανάλια κοινωνικών μέσων: Χρήση πλατφορμών κοινωνικών μέσων για τη διάδοση της ευαισθητοποίησης και την προσέγγιση ενός ευρύτερου κοινού.

c. Εκπαίδευση για την ασφάλεια στο διαδίκτυο:

- Διαδικτυακά σεμινάρια και εργαστήρια: Διοργάνωση διαδικτυακών εκπαιδευτικών συνεδριών και εκδηλώσεων όπου οι ειδικοί στον τομέα της ασφάλειας στον κυβερνοχώρο παρέχουν πρακτικές συμβουλές και απαντούν σε ερωτήσεις πελατών.
- Προσομοιώσεις και δοκιμές: Εφαρμογή προσομοιώσεων ηλεκτρονικού "ψαρέματος" για να διδάξετε στους πελάτες πώς να εντοπίζουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου και μηνύματα.

d. Υποστήριξη πελατών:

- Γραμμές βοήθειας: Παροχή ειδικής τηλεφωνικής γραμμής όπου οι πελάτες μπορούν να αναφέρουν ύποπτα περιστατικά και να λαμβάνουν άμεση υποστήριξη.
- Εξατομικευμένες συμβουλές: Παροχή εξατομικευμένων συμβουλών και υποστήριξης για πελάτες που χρειάζονται βοήθεια για τη διαχείριση της ασφάλειας των ηλεκτρονικών λογαριασμών τους.

e. Ενημερώσεις ασφαλείας και προειδοποιήσεις:

- Ειδοποιήσεις ασφαλείας: Αποστολή ειδοποιήσεων μέσω email ή μηνυμάτων κειμένου όταν εντοπίζεται ύποπτη δραστηριότητα στον λογαριασμό του πελάτη ή όταν εμφανίζονται νέες απειλές.
- Επικαιροποιημένες πληροφορίες: Διατηρήστε μια ενότητα στον ιστότοπο της τράπεζας με τα τελευταία νέα και συμβουλές στον τομέα της κυβερνοασφάλειας.

Μέσω αυτών των μέτρων, τα χρηματοπιστωτικά ιδρύματα όχι μόνο προστατεύουν τους δικούς τους πόρους, αλλά συμβάλλουν επίσης στη δημιουργία ασφαλέστερου χρηματοπιστωτικού περιβάλλοντος για όλους τους χρήστες. Η εκπαίδευση και η συνεχής συνεργασία με τους πελάτες, μαζί με την εφαρμογή των τελευταίων τεχνολογιών ασφάλειας, είναι απαραίτητες για την καταπολέμηση της οικονομικής απάτης. Αυτή η συνδυασμένη προσέγγιση συμβάλλει στην οικοδόμηση εμπιστοσύνης στο χρηματοπιστωτικό σύστημα και στην αποτελεσματική προστασία των περιουσιακών στοιχείων των πελατών από απειλές στον κυβερνοχώρο.

Ως εκ τούτου, ο ρόλος των χρηματοπιστωτικών ιδρυμάτων είναι κρίσιμος όχι μόνο για την αποτελεσματική διαχείριση των οικονομικών, αλλά και για τη διασφάλιση ενός ασφαλούς και προστατευμένου περιβάλλοντος για τις χρηματοπιστωτικές συναλλαγές στην ψηφιακή εποχή. Μέσω της στενής συνεργασίας με τις ρυθμιστικές αρχές, άλλα ιδρύματα και πελάτες, μπορούν να συνεχίσουν να βελτιώνουν την άμυνα κατά της εξελιγμένης οικονομικής απάτης.

7. Σχέδιο αντιμετώπισης συμβιβασμών

Άμεση δράση μετά τον εντοπισμό απάτης

a. Κοινοποίηση των χρηματοπιστωτικών ιδρυμάτων:

Επικοινωνήστε αμέσως με την εμπλεκόμενη τράπεζα ή χρηματοπιστωτικό ίδρυμα. Η ακύρωση ή ο άμεσος αποκλεισμός οποιωνδήποτε πιστωτικών/χρεωστικών καρτών και η ηλεκτρονική πρόσβαση σε λογαριασμούς είναι ζωτικής σημασίας για την πρόληψη περαιτέρω απωλειών.

b. Αλλάξτε τα διαπιστευτήρια σύνδεσής σας:

Αλλάξτε τους κωδικούς πρόσβασης και τις λεπτομέρειες ασφαλείας για όλους τους ηλεκτρονικούς λογαριασμούς που επηρεάζονται. Αυτό περιλαμβάνει λογαριασμούς ηλεκτρονικού ταχυδρομείου, πλατφόρμες κοινωνικών μέσων και οποιαδήποτε σχετική διαδικτυακή υπηρεσία.

c. Υποβολή εκθέσεων στις αρμόδιες αρχές:

Αναφέρετε την απάτη στην αστυνομία, στην Εθνική Διεύθυνση Ασφάλειας στον Κυβερνοχώρο και σε άλλες σχετικές αρχές, όπως η εθνική εποπτική αρχή για τη χρηματοοικονομική απάτη. Μπορεί να βοηθήσει στη διερεύνηση και την πρόληψη άλλων παρόμοιων περιπτώσεων.

d. Παρακολούθηση πιστώσεων:

Σε περίπτωση κλοπής ταυτότητας, είναι σημαντικό να παρακολουθείτε τις πιστωτικές σας αναφορές για οποιαδήποτε μη εξουσιοδοτημένη δραστηριότητα. Οι υπηρεσίες παρακολούθησης πιστώσεων μπορεί να θεωρηθεί ότι ειδοποιούν για τυχόν ύποπτες αλλαγές.

Ανάκτηση ζημιών και εξασφάλιση λογαριασμών

a. Διατήρηση αποδεικτικών στοιχείων:

Αποθηκεύστε όλες τις συζητήσεις, τα έγγραφα, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, τους αριθμούς τηλεφώνου των ατόμων με τα οποία αλληλεπιδράσατε. Αποφύγετε τη διαγραφή εγκατεστημένων εφαρμογών ή συσκευών μορφοποίησης που εμπλέκονται στο περιστατικό.
Οι πληροφορίες μπορούν να βοηθήσουν στον προσδιορισμό του τρόπου με τον οποίο διαπράχθηκε η απάτη, αλλά και της ταυτότητας των εγκληματιών.

b. Έλεγχος συναλλαγών:

Ελέγξτε όλες τις πρόσφατες συναλλαγές για μη εξουσιοδοτημένη δραστηριότητα. Αυτό θα βοηθήσει στον προσδιορισμό του επιπέδου συμβιβασμού.

c. Λεπτομερής τεκμηρίωση και αναφορά του συμβάντος:

Διατηρήστε λεπτομερές αρχείο όλων των επικοινωνιών και των ενεργειών που πραγματοποιούνται μετά τον εντοπισμό απάτης. Αυτό περιλαμβάνει οποιαδήποτε αναφορά στην αστυνομία, αλληλογραφία με την τράπεζα και αλλαγές ασφαλείας που έγιναν.

d. Διαβούλευση με οικονομικό ή νομικό εμπειρογνώμονα:

Σε περίπλοκες περιπτώσεις, μπορεί να είναι χρήσιμο να συμβουλευτείτε έναν οικονομικό ή νομικό εμπειρογνώμονα για να σας καθοδηγήσει στη διαδικασία ανάκτησης ζημιών και προστασίας των δικαιωμάτων σας.

e. Επαναξιολόγηση των μέτρων ασφαλείας:

Επανεξέταση και βελτίωση των πρακτικών ασφαλείας για την πρόληψη παρόμοιων περιστατικών στο μέλλον. Αυτό μπορεί να περιλαμβάνει την επένδυση σε πιο προηγμένες λύσεις ασφάλειας, την αναθεώρηση των πολιτικών ασφάλειας και την ευαισθητοποίηση σχετικά με την προστασία των δεδομένων.

8. Συμπέρασμα

Η σημασία της ευαισθητοποίησης και της πρόληψης

" ευαισθητοποίηση και η πρόληψη είναι ουσιαστικής σημασίας για την καταπολέμηση της οικονομικής απάτης. Σε έναν ολοένα και πιο ψηφιοποιημένο κόσμο, όπου οι χρηματοπιστωτικές συναλλαγές πραγματοποιούνται σε μεγάλο βαθμό στο διαδίκτυο, οι δυνατότητες παράνομων δραστηριοτήτων ενισχύονται. Ως εκ τούτου, είναι ζωτικής σημασίας τόσο τα άτομα όσο και τα χρηματοπιστωτικά ιδρύματα να είναι καλά ενημερωμένα και να λαμβάνουν προληπτικά μέτρα για την προστασία τους από αυτές τις απειλές.

Ο ρόλος της ευαισθητοποίησης:

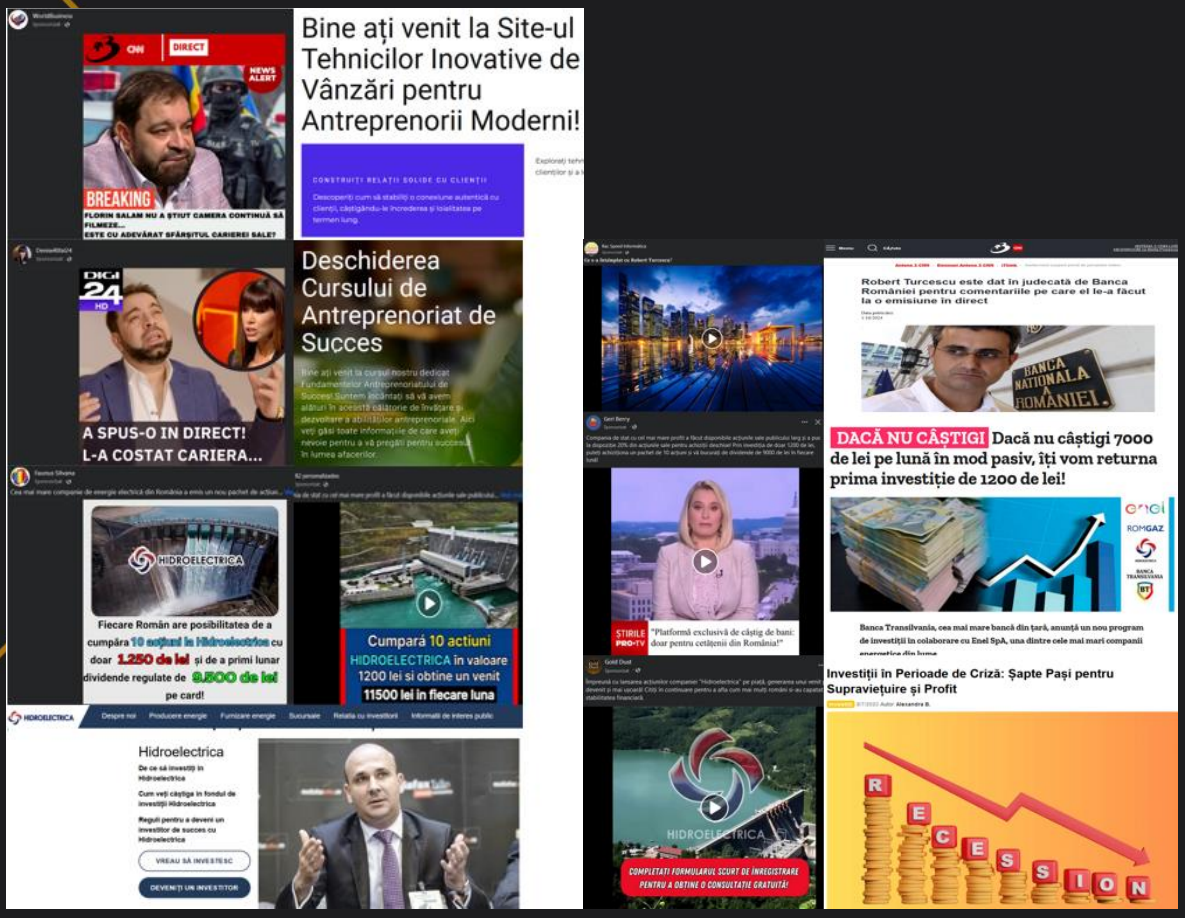
- **Εκπαίδευση: Η** καλή ενημέρωση σχετικά με τους διάφορους τύπους οικονομικής απάτης και τα προειδοποιητικά σημάδια τους μπορεί να κάνει τη διαφορά μεταξύ του να είσαι θύμα και να αποτρέπεις μια επίθεση. Η συνεχής εκπαίδευση είναι ζωτικής σημασίας για να συμβαδίζει με τις συνεχώς μεταβαλλόμενες μεθόδους των παραβατών.
- **Ανταλλαγή πληροφοριών: Η** διάδοση προσωπικών γνώσεων και εμπειριών που σχετίζονται με την οικονομική απάτη στις κοινότητες μπορεί να συμβάλει στην αύξηση της γενικής ευαισθητοποίησης και στην προστασία των άλλων.

Η σημασία της πρόληψης:

- **Μέτρα ασφαλείας:** Η εφαρμογή αυστηρών μέτρων ασφαλείας, τόσο σε προσωπικό όσο και σε θεσμικό επίπεδο, είναι απαραίτητη για τον αποκλεισμό της πρόσβασης των εγκληματιών σε πληροφορίες και οικονομικούς πόρους.
- **Συνεχής επαγρύπνηση:** Η διατήρηση μιας στάσης επαγρύπνησης και η τακτική επανεξέταση των πρακτικών ασφαλείας διασφαλίζει ότι είμαστε πάντα ένα βήμα μπροστά από τους εγκληματίες.

Τέλος, η πρόληψη και η καταπολέμηση της οικονομικής απάτης αποτελεί κοινή ευθύνη. Μέσω της συνεργασίας μεταξύ καταναλωτών, χρηματοπιστωτικών ιδρυμάτων και ρυθμιστικών αρχών, μπορούμε να οικοδομήσουμε ένα ασφαλέστερο και πιο προστατευμένο χρηματοπιστωτικό περιβάλλον. Η ευαισθητοποίηση σχετικά με τους κινδύνους και τα προληπτικά μέτρα ασφαλείας δεν αποτελούν μόνο εγγύηση έναντι οικονομικών απωλειών, αλλά και ουσιαστικό βήμα προς τη διατήρηση μιας ασφαλούς και σίγουρης ψηφιακής κοινωνίας.

9. Μπόνους: Συνεχιζόμενες εκστρατείες απάτης



Πηγές και περαιτέρω ανάγνωση

Phishing επίθεση – **Cyber AID**
https://www.cyberaid.eu/atacul-de-tip-phishing/

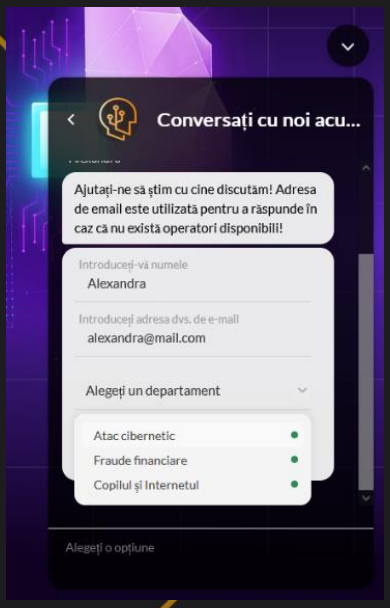
Bank Phishing – Ασφάλεια **στο Internet**
https://sigurantaonline.ro/phishing-ul-bancar/

Άρθρα για την ασφάλεια στον κυβερνοχώρο - **Prodefence**
https://www.prodefence.ro/articole-securitate-cibernetica/

Ανίχνευση ηλεκτρονικής απάτης - **DNSC**
https://www.dnsc.ro/cautare?ceCaut=frauda

Cyber Intelligence – Χρήση προφίλ – **ISACA | DNSC**
https://dnsc.ro/vezi/document/isaca-cyber-intelligence-using-profiling/

Cyber Edequation – Γονείς και Παιδιά – **Prodefence**
https://www.youtube.com/@AlexandruAnghelus/videos



Διαδικτυακή συνομιλία

Πριν στείλετε προσωπικά δεδομένα ή χρήματα σε έναν ξένο, είναι προτιμότερο να ζητήσετε τη γνώμη ειδικών. Είναι δωρεάν και μπορώ να σας βοηθήσω να μην πάρετε λάθος αποφάσεις!

https://www.cyberaid.eu/ | https://sigurantadigitala.ro/

Διατίθεται μόνο στα ρουμανικά!

"Λέτε ότι όλα είναι ψέματα και είναι όλοι κλέφτες, αλλά δίνετε όλα τα προσωπικά σας δεδομένα και τα χρήματά σας σε ένα άτομο που σας είπε ιστορίες μέσω μηνύματος ή τηλεφώνου"

ProDefence

Cyber Security Services