Κοινωνική Μηχανική (Social Engineering)

Ο όρος Κοινωνική μηχανική (Social engineering) αναφέρεται στην ψυχολογική χειραγώγηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών.

Πρόκειται για ένα σύνολο διαδοχικών βημάτων και σταδίων που αφορούν συλλογή πληφοριών, τεχνάσματα και εξαπάτηση φυσικών προσώπων, με τελικό σκοπό την **πρόσβαση σε κάποιο υπολογιστικό πληφορορiακό σύστημα**.

Συνήθως αυτός που την εφαρμόζει δεν έρχεται ποτέ σε άμεση επαφή με τα άτομα που εξαπατά ή παραπλανά, χωρίς αυτό να συνιστά γενικόν κανόνα.

Ο πρώην hacker και αργότερα σύμβουλος ασφαλείας πληροφορικών συστημάτων **Κέβιν Μίτνικ**, ήταν από τους πρώτους που διέδωσαν τον όρο «κοινωνική μηχανική», επισημαίνοντας ότι *είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να δώσει έναν κωδικό πρόσβασης για ένα σύστημα από το να προσπαθήσεις να τον σπάσεις*

Ο όρος **Κοινωνική Μηχανική** αναφέρεται και στις κοινωνικές επιστήμες, όμως έχει πλέον καθιερωθεί από τους επαγγελματίες της ασφάλειας πληροφοριακών συστημάτων.

Η συμπεριφορά των εργαζομένων σε έναν οργανισμό, έχει τεράστιο αντίκτυπο στην ασφάλεια πληροφοριών. Η έννοια της κουλτούρας απέναντι σε μια δέσμη συμπεριφορών, δύναται να συμβάλλει αποτελεσματικά στην επιτυχία της ασφάλειας πληροφορίας ενός οργανισμού. Στην πραγματικότητα η κουλτούρα τρόπων συμπεριφοράς του προσωπικού, οδηγεί από μόνη της στην εξασφάλιση και προστασία κάθε μορφής πληροφορίας.

Οι Anderson, D., Reimers, K. και Barretto, C. (2014) βρήκαν πως το προσωπικό ενός οργανισμού συνήθως δεν θεωρεί τον εαυτό του ως μέρος της ασφάλειας πληροφοριών. Απαιτείται επομένως εκπαίδευση, αξιολόγηση, εκπαίδευση κι επαναξιολόγηση, ώστε να αποκτηθεί η κουλτούρα της ασφάλειας μέσα στη συμπεριφορά του προσωπικού.

Η **Προ-αξιολόγηση**, καθορίζει το βαθμό εγρήγορσης για την ασφάλεια πληφορορiών στο προσωπικό και αναλύει την ήδη υπάρχουσα πολιτική ασφαλείας.

Η **Στρατηγική Σχεδίαση**, σχεδιάζει ένα πρόγραμμα που θα οδηγήσει σε μεγαλύτερη εγρήγορση. Οι στόχοι είναι σαφείς: τα ομαδικά και δημοφιλή στελέχη ενός οργανισμού. Αυτοί θα συμβάλλουν όσο κανείς άλλος στην υλοποίηση του προγράμματος.

Η **Λειτουργική Σχεδίαση**, περιλαμβάνει όλες εκείνες τις ενέργειες που θα βελτιώσουνι την εσωτερική επικοινωνία, την υιοθέτηση και ενσωμάτωση στη Διοίκηση, καθώς και την εκπαίδευση του προσωπικού για εγρήγορση ως προς την ασφάλεια πληροφοριών.

Η **Υλοποίηση** περιλαμβάνει τα τέσσερα στάδια που θα εγκαθιδρύσουν κουλτούρα ασφαλείας σε έναν οργανισμό. Αυτά είναι η υποχρέωση της Διοίκησης, η επικοινωνία των τμημάτων του οργανισμού, η οργάνωσή τους και τέλος η ενσωμάτωση στο προσωπικό.

Τεχνικές και Ορολογία

Οι τεχνικές

Όλες οι τεχνικές βασίζονται στις συνήθη σεμπεριφορά του ανθρώπου όταν πρόκειται να πάρει αποφάσεις και είναι γνωστές ως γνωστικές προκαταλήψεις (cognitive biases).

Συχνά αυτές οι προκαταλήψεις (bugs στο ανθρώπινο hardware) χρησιμοποιούνται συνδυαστικά, ώστε να δημιουργήσουν έδαφος για επιθέσεις. Ο συχνότερος τρόπος για επιθέσεις κοινωνικής μηχανικής είναι το τηλέφωνο, ενώ δεν εκλείπουν και επιθέσεις φυσικής παρουσίας.

Τεχνικές Κοινωνικής Μηχανικής

Σενάριο / Pretexting

Επινόηση σεναρίου, ώστε να προσεγγίσει ο επιτιθέμενος το θύμα.

α) Αρχικά κάνει μια **έρευνα** (συχνά στα “σκουπίδια”) ώστε να γίνει γνώστης πραγματικών πληροφοριών που αφορούν το θύμα, ώστε στη συνέχεια προσεγγίζοντάς το να κερδίσει την εμπιστοσύνη του. Πχ ημερομηνία γέννησης, αριθμός / είδος κοινωνικής ασφάλισης, μέλος σωματείων ή συλλόγων, φίλοι από κοινωνικά δίκτυα, λογαριασμός από κάποια δραστηριότητα κοκ.

β) **Προσέγγιση** του θύματος προσποιούμενος ότι είναι κάποιος γνωστός. Με αυτόν τον τρόπο, το θύμα υποσυνείδητα θεωρεί το πρόσωπο του επιτιθέμενου νόμιμο, καθαρό, επίσημο, δίνοντάς του πιστότητα, που υπό κανονικές συνθήκες δεν θα του έδινε.

Συχνά πχ δεν θέλουμε να δείξουμε ότι δεν θυμόμαστε κάποιον. Έτσι ο επιτιθέμενος προσποιείται ότι είναι κάποιος από το πρόσφατο, άμεσο φιλικό περιβάλλον μας, τον οποίο εμείς παραβλέψαμε ή δεν θυμόμαστε. Για να μας πείσει αναφέρεται σε πραγματικά περιστατικά με πραγματικές λεπτομέρειες, τις οποίες διαθέτει, μετά από διεξαγωγή έρευνας.

Σενάριο / Pretexting (συνέχεια)

γ) **Σενάριο**. Στη συνέχεια ο επιτιθέμενος κατασκευάζει ένα σενάριο, με πιθανές ερωτήσεις του υποψηφίου θύματος, στις οποίες προετοιμάζει τις απαντήσεις του.

Όσο περισσότερο επεξεργαστεί αυτό το σημείο, τόσο περισσότερες πιθανότητες έχει να επιτύχει το στόχο του. Οι γρήγορες, με σταθερό τόνο, αυτοπεποιήθηση και ύφος επισημότητας απαντήσεις, συνήθως πείθουν το υποψήφιο θύμα.

Υπενθυμίζεται πως τα βήματα (α) και (β), αν είναι καλά προετοιμασμένα, το υποψήφιο θύμα είναι πρόθυμο να απαντήσει, καθώς έχει προηγουμένως καλλιεργηθεί κλίμα φιλίας κι εμπιστοσύνης.

Πρόκληση Παράκαμψης, Αλλαγή ροής / Diversion theft

Ο επιτιθέμενος, παρεμβαίνει ώστε να προκαλέσει μια παράκαμψη, ή αλλαγή ροής, σε μια νόμιμη και συνήθη διαδικασία, ώστε να φέρει το υποψήφιο θύμα σε μια κατάσταση, όπου δεν θα είναι προετοιμασμένο να ανταποκριθεί.

Η αλλαγή αυτή στη φυσική / συνήθη ροή, προκαλείται συνήθως από μια τεχνιτή βλάβη, ή ψευδές απροειδοποίητο δήθεν συμβάν που εμποδίζει τη φυσική ροή.

Έτσι το θύμα οδηγείται σε μια κατάσταση, όπου έχει άγνοια, αισθάνεται άβολα και θέλει βοήθεια. Είναι λοιπόν πρόθυμο να την δεχθεί και να πειθαρχήσει σε κάποιον που θα του παρουσιαστεί ως έμπειρος μιας τέτοιας κατάστασης, παραθέτοντάς του πραγματικά περιστατικά.

Ψάρεμα / Phishing

Ο επιτιθέμενος χρησιμοποιεί τεχνικές εξαπάτησης, ώστε να αποσπάσει από το θύμα πληφορίες ή να το οδηγήσει στο να πράξει ασυνήθιστα.

α) Πλημμυρίδα emails ανεπίκλητης αλληλογραφίας (**spams**). Επιτίθεται μαζικά σε στελέχη μιας εταιρείας. Κάποιοι θα ανταποκριθούν με λάθος τρόπο (θα “τσιμπήσουν”), κι ο επιτιθέμενος θα έχει κάνει ένα σημαντικό βήμα. (επιτυχία 5% συνήθως)

β) **Στοχευμένη επίθεση** σε κάποια στελέχη. Η αλληλογραφία είναι προσωποποιημένη, αφορά δήθεν εκκρεμότητες του θύματος με τράπεζα ή εφορία ή τον υπολογιστή του που σέρνεται, ότι βρέθηκε στον υπολογιστή του άσεμνο υλικό και η συζήτηση θα έπρεπε να είναι εμπιστευτική, ότι ο Διευθυντής ή ο Υποδιευθυντής συνηγόρησαν αρνητικά για τον ίδιο σε μια συγκεκριμένη ενέργειά του και η οποία θα μπορούσε να διορθωθεί (“έχει ξαναγίνει και με τον δείνα”) κοκ (επιτυχία 50% συνήθως)

Πλημμυρίδα ανεπίκλητης αλληλογραφίας (mail **spam**)

1) “...ένας που δεν έστειλε, τραυματίστηκε σε τροχαίο, η σύζυγος του υποδιοικητή της αστυνομίας απέβαλε. Ο περιπτεράς της γωνίας γέλασε, αλλά τον έσπασαν στο ξύλο και τον λήστεψαν.” κοκ

2) “… ξέρω ότι με θέλεις και ντρέπεσαι να μου το πεις… ξέρεις σε θέλω κι εγώ και φοβάμαι… είμαι η/ος. Θα ήθελα να επικοινωνούμε με ψευδώνυμα: εγώ θα υπογράφω ως κόκκινο τριαντάφυλλο, ενώ εσύ ως Χαμένος ταξιδευτής”.

Πλημμυρίδα ανεπίκλητης αλληλογραφίας (mail **spam**) – συνέχεια.

3). Ένας λαμβάνει ένα email από έναν άγνωστο που τον ενημερώνει ότι έχει επαφή με τα στημμένα στοιχήματα. Χρόνια συμμετείχε, κέρδισε, αλλά τώρα απηύδησε και θα ήθελε να βοηθήσει μερικούς φτωχούς σαν κι εκείνον. Τον καλεί να παίξει ένα μικρό ποσό για να πειστεί. Το θύμα παίζει και κερδίζει. Στη συνέχεια του λέει να παίξει ένα άλλο στοίχημα τα κερδισμένα. Το θύμα ανταποκρίνεται και κερδίζει. Στη συνέχεια του ξαναστέλνει μήνυμα καλώντας τον για ένα χοντρό στοίχημα. Το θύμα ανταποκρίνεται και κερδίζει. Τέλος τον καλεί για ένα ακόμη πιο δυνατό και κερδοφόρο στοίχημα. Το θύμα ανταποκρίνεται και χάνει όλα τα κερδισμένα, καθώς και άλλα τόσα.

Ψάρεμα / Phishing με φωνή από τηλέφωνο

Το θύμα δέχεται αυτοματοποιημένο τηλεφώνημα δήθεν από την εταιρεία του ή την τράπεζά του, όπου το καλούν να ανταποκριθεί με σκοπό να επιλυθούν κάποια επιμέρους ζητήματά του, να διευθετηθεί κάποιο δάνειό του κλπ.

“Τρύπα στο νερό” / Water hooling

Συλλέγονται πληροφορίες για ένα θύμα σχετικά με ποιές ιστοσελίδες επισκέπτεται συχνά και τις οποίες εμπιστεύεται.
Γίνεται έρευνα για το ποιές από αυτές είναι ευάλωτες και ευεπίφορες για κακόβουλο λογισμικό, το οποίο θα εγχεθεί στο θύμα.
Στήνεται η παγίδα, που έχει την όψη απλού νερόλακκου…

Δόλωμα / Baiting

Εδώ γίνεται εκμετάλλευση της περιέργειας ή της απληστίας των θυμάτων. Κατασκευάζονται DVDs ή USB memory sticks, τα οποία έχουν δήθεν έγγραφα με ονόματα από λογότυπο της εταιρείας-στόχου με και ελκυστικούς τίτλους (πχ μισθοδοσία διευθυντικού προσωπικού, Άκρως Απόρρητο κα) και αφήνονται σε ανελκυστήρες, σε μπαρ, σε καφέ ή όπου αλλού συχνάζουν στελέχη της εταιρείας

Αυτός που θα το πάρει θα το συνδέσει και πολύ πιθανόν να μολυνθεί, προδίδοντας πρόσβαση στους επιτιθέμενους.

Για καθέναν, υπάρχει κάποιος κάπου / Quid pro quo

Αθρόα τηλεφωνήματα από τον επιτιθέμενο σε τυχαίους αριθμούς μιας εταιρείας. Ο επιτιθέμενος ισχυρίζεται ότι είναι από το τεχνικό τμήμα και ότι πήρε κλήση από τον συγκεκριμένο αριθμό για κάποιο τεχνικό πρόβλημα με τον υπολογιστή, γι' αυτό και καλεί πίσω. Κάποιο από αυτά τα τυχαία νούμερα είναι πολύ πιθανόν να οδηγήσει σε στέλεχος που πραγματικά έχει κάποιο πρόβλημα. Το στέλεχος χαίρεται που επιτέλους κάποιος είναι πρόθυμος να τον βοηθήσει, έτσι είναι κι ο ίδιος πρόθυμος να συνεργαστεί με τον επιτιθέμενο.

"Μαντέψτε τον μυστικό κωδικό! Κερδίστε μια πολυτελή πένα καλλιγραφίας". Πολλοί που ανταποκρίθηκαν σε έρευνες και μελέτες έδωσαν είτε τους ίδιους τους κωδικούς τους, είτε τμήματά των.

Ακριβώς πίσω από κάποιον / Tailgating

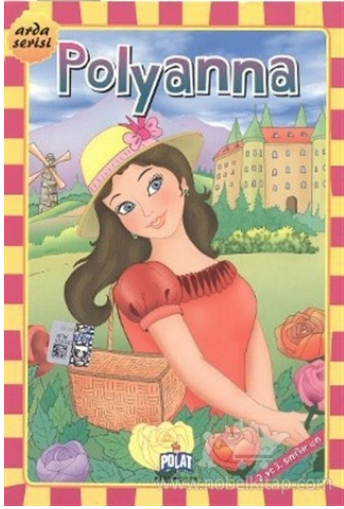
Αυτή η τεχνική χρησιμοποιείται για λαθραία είσοδο σε προστατευμένες περιοχές όπου υπάρχει αυτόματο σύστημα πρόσβασης (πχ με ηλεκτρονική κάρτα εισόδου) ανεπιτήρητο.

Ο επιτιθέμενος, ακολουθεί ακριβώς από πίσω, ένα νόμιμο στέλεχος και μπαίνει μαζί του. Συχνά για λόγους αβρότητας το ανυποψίαστο νόμιμο στέλεχος μπορεί να κρατήσει και την πόρτα ανοικτή στον επιτιθέμενο ή και να ζητηθεί από τον επιτιθέμενο ευγενικά στο νόμιμο στέλεχος να κρατήσει την πόρτα. Το στέλεχος σπάνια θα ρωτήσει για την ταυτότητα του επιτιθέμενου, ιδίως εάν έχει όψη και εικόνα καλοβαλμένου στελέχους της εταιρείας. Στην περίπτωση που θα ρωτήσει, ο επιτιθέμενος μπορεί να ισχυριστεί ότι ξέχασε την κάρτα του.

Ενίοτε ο επιτιθέμενος, μπορεί να υποκριθεί ότι χρησιμοποίησε κι αυτός την (ανύπαρκτη) κάρτα του.

Στοιχεία της Κοινωνικής Μηχανικής

- Άνθρωποι
- Υπολογιστικά συστήματα



From Nov. 12, 2001 Fortune Magazine

"Ask Annie" Column

Αγαπητή Άννα,

Ασχολούμαι με την έρευνα αγοράς που επιπλέον περιλαμβάνει και πληροφορίες για ανταγωνιστές μας, για μια μικρή εταιρεία πληροφορικής. Κυρίως από το ίντερνετ, από άρθρα στον Τύπο, από επίσημες βιομηχανικές επαφές ή βιομηχανικές αναφορές που αγοράζουμε. Τώρα το αφεντικό μου θέλει να αρχίσω να καλώ τους μεγαλύτερους ανταγωνιστές μας, υποκρινόμενη ότι επιθυμώ να είμαι μεταπωλήτρια των προϊόντων/υπηρεσιών τους, ώστε να αποκτήσω έμπιστες πληροφορίες για προϊόντα και μελλοντικό σχεδιασμό τους. Δεν μου φαίνεται πολύ ηθικό αυτό. Είμαι μια αθώα **Πολυάννα**? Το κάνουν όλοι αυτό?

- *Squeamish in Seattle*

Η Κοινωνική Μηχανική στοχεύει σε βασικά στοιχεία του χαρακτήρα της ανθρώπινης φύσης:

- Την επιθυμία να βοηθάμε τους γύρω μας και να φαινόμαστε χρήσιμοι
- Την τάση να εμπιστευόμαστε τους ανθρώπους
- Τον φόβο να μην μπλέξουμε σε μπελάδες.

Ο πραγματικά επιτυχημένος αυτουργός της Κοινωνικής Μηχανικής δεν δημιουργεί καμία υποψία.

Εναλλακτικοί Τρόποι πειθούς:

- Άμεσος Τρόπος. Οργάνωση λογικών επιχειρημάτων. Στοχεύει στη **λογική** ώστε να πείσει.

- Πλάγιος Τρόπος. Πλάγια και έμμεση αναφορά στα επιμέρους. Στοχεύει σε υποσυνείδητους **συναισθηματικούς** αυτοματισμούς, δεν αναφέρει ρητά τους σκοπούς και τους στόχους, ώστε να προκαλέσει την αποδοχή χωρίς πολλή σκέψη.

Στοχεύοντας στα συναισθήματα:
Η επιστράτευση γίνεται με μικρή σχεδόν ανεπαίσθητη νύξη σε ζητήματα που προκαλούν ισχυρή έκλυση συναισθημάτων.

- Πρόκληση αδιόρατου ενθουσιασμού.
- Πρόκληση αδιόρατου φόβους πολλή σκέψη.

Ο Γενικός Διευθυντής είναι στην άλλη γραμμή και περιμένει άμεσα την πληροφορία!

Εναλλακτικοί Τρόποι πειθούς:

Βιάζομαι σήμερα, γιατί περιμένει ο γενικός του τμήματος προσωπικού την έκθεση αξιολόγησης του προσωπικού. Έχω ήδη αργήσει.

(… μικρή παύση… αλλαγή ύφους)

Αλήθεια πως ονομάζεστε? Ποιος είναι ο αριθμός μητρώου σας? Να σας πω λίγα λόγια σχετικά με εσάς και το πώς σας έχουμε αξιολογήσει.

Εναλλακτικοί Τρόποι πειθούς:

Οι άνθρωποι έχουν την τάση να εμπιστεύονται τους συνανθρώπους τους, ιδίως τους «ομοιοπαθείς», συναδέλφους, συνεργάτες κλπ.

Έτσι παραβλέπουν τα πρωτόκολλα, τις τυποποιημένες ενέργειες κλπ.

Η Κοινωνική Μηχανική διακρίνεται σε:

Ανθρώπινη Διεπαφή. Υπάρχει φυσική και σε πραγματικό χρόνο διεπαφή ώστε να αποσπαστεί η πληροφορία.

Διεπαφή υπολογιστικών μηχανών. Χρησιμοποιείται λογισμικό το οποίο θα υποκλέψει τις πληροφορίες.

Ανθρώπινη Διεπαφή. Οι μελέτες έχουν δείξει ότι συχνότεροι στόχοι επιθέσεων είναι τα help desks.

Πλαστοπροσωπεία.
Ο επιτιθέμενος καλεί το helpdesk**.** Τα Helpdesk είναι από τη φύση τους, εξυπηρετικά προς το προσωπικό. Ο επιτιθέμενος γνωρίζει ονόματα και πρόσωπα της εταιρείας. Συνήθως λόγω φόρτου εργασίας τα helpdesk δεν κάνουν αναγνώριση της ταυτότητας του καλούντος.

Σημαντικός Χρήστης. Ο επιτιθέμενος υποκρίνεται ότι είναι ένας Γενικός Διευθυντής σε κάποιο σημαντικό τμήμα – κατά προτίμηση άσχετο με την τεχνολογία. Το helpdesk δύσκολα θα αρνηθεί να εξυπηρετήσει ένα υψηλά ιστάμενο στέλεχος της εταιρείας. Ο επιτιθέμενος μπορεί να απειλήσει να αναφέρει τον εργαζόμενο στον προϊστάμενό του.

Συνεργαζόμενος οργανισμός.
Ο επιτιθέμενος υποκρίνεται ότι είναι ένας έγκυρος κι επίσημος εκπρόσωπος ενός καλά εγκαθιδρυμένου στην εταιρεία στόχο, τρίτου συνεργαζόμενου οργανισμού, ο οποίος υπό κανονικές συνθήκες από καιρόν εις καιρόν έχει πρόσβαση στις εμπιστευτικές πληροφορίες.

Τεχνική Υποστήριξη. Ο επιτιθέμενος υποκρίνεται ότι είναι υπάλληλος της τεχνικής υποστήριξης.

Το σύστημα έχει παρουσιάσει δυσλειτουργίες. Παρακαλούμε όλο το προσωπικό να βγεί από το σύστημα και να επανεκκινήσει τους υπολογιστές του. Θα σας τηλεφωνήσω για να μπείτε.

Φυσική Πρόσβαση. Ο επιτιθέμενος μπαίνει και περιπλανάται στους χώρους μιας εταιρίας, υποκρινόμενος ότι είναι υπάλληλος, επισκέπτης ή τεχνικός συντήρησης.

Κατάλληλη εμφάνιση / ενδυμασία, ανάλογα το ρόλο.

Μπορεί επίσης να ενσωματωθεί στο προσωπικό **καθαρισμού.** Το οποίο μπαίνει σχεδόν σε όλους τους χώρους.

Προσωπικότητα. Ο επιτιθέμενος εκμεταλλεύεται στοιχεία της προσωπικότητας του εργαζόμενου ώστε να επιτύχει την απόσπαση των πληροφοριών που τον ενδιαφέρουν.

Διάχυση της ευθύνης. Το θύμα πείθεται ότι δεν είναι αποκλειστικά υπεύθυνο ώστε αν πράξει όπως τον προτρέπουν, δεν θα είναι ο μόνος υπαίτιος.

Ο επιτιθέμενος παρουσιάζει το ζήτημα έτσι ώστε να θέτει στο θύμα και άλλα ονόματα που επίσης είναι υπεύθυνοι και έπραξαν ανάλογα. Μπορεί ακόμη να επιστρατεύσει και το όνομα κάποιου από τα υψηλά στελέχη της εταιρείας, λέγοντας ότι συνηγορεί για κάτι τέτοιο.

Ευκαιρία Εύνοιας. Το θύμα παραπλανάται, έτσι ώστε να πιστεύει ότι εξυπηρετώντας τον επιτιθέμενο, αποκτάει ευκαιρίες:

-Θα έχει εύνοια από τον προϊστάμενό του, έναντι ανταγωνιστών συναδέλφων του.

-Θα έχει καλό όνομα στη διοίκηση

-Θα εξυπηρετήσει μια θελκτική όμορφη συνάδελφο.

Σχέσεις Εμπιστοσύνης. Ο επιτιθέμενος καλλιεργεί σχέσεις εμπιστοσύνης και αλληλοβοήθειας με το υποψήφιο θύμα του. Πχ κάνοντας διάφορες μικρές «εξυπηρετήσεις» σε αυτόν.

Ηθικό Καθήκον. Το θύμα πείθεται ότι ενεργώντας με συγκεκριμένο τρόπο επιτελεί ένα ηθικό καθήκον ή διορθώνει μια αδικία, ή αποδοκιμάζει μια ηθική προσβολή κάποιου αγαπητού του προσώπου.

Απαιτείται αρκετή συλλογή παράπλευρων πληροφοριών για τη διενέργεια και επιστράτευση μιας τέτοιας βάσης.

Το θύμα πείθεται ότι ένα λάθος ή ένα κακό έχει συμβεί και ενεργώντας έτσι θα μετριάσει τις αρνητικές συνέπειες.

Ενοχές. Οι περισσότεροι έχουν την τάση να αποδιώχνουν τα συναισθήματα που προκαλούν ενοχές. Έτσι ο επιτιθέμενος πείθει το θύμα ότι ενεργώντας με αυτόν τον τρόπο, δεν θα είναι συνένοχος σε κάτι.

Ταύτιση. Ο επιτιθέμενος καλλιεργεί σχέσεις ταύτισης με το θύμα. Η αναγνώριση και η ταύτιση μεταξύ δυο ανθρώπων αποδιώχνουν την τυπικότητα στη συμπεριφορά.

Επιθυμία για βοήθεια. Ο επιτιθέμενος εκμεταλλεύεται την ορμέμφυτη τάση να βοηθάμε τους συνανθρώπους μας. Έτσι συνήθως:
-Ανοίγουμε μια πόρτα
-Βοηθάμε κάποιον να μπει σε έναν λογαριασμό.
-Είμαστε αβέβαιοι ή δύσκολα λέμε όχι.

Συνεργασιμότητα. Δεν επιθυμούμε διαμάχες και σκιαμαχίες. Ο επιτιθέμενος επιστρατεύει κι επιδεικνύει πνεύμα συνεργασίας. Επικαλείται:

- Τη φωνή της λογικής
- Την δήθεν φυσική ροή των πραγμάτων σε μια άγνωστη κατάσταση
- Είναι υπομονετικός
- Τονίζει τα θετικά, μην λησμονώντας να υπενθυμίσει τις υποτιθέμενες αρνητικές συνέπειες που θα εγκύψουν για το θύμα του, αν δεν συνεργαστεί.

ΑΙΤΗΜΑΤΑ που τίθενται από τον επιτιθέμενο.

Άμεσα. Αποφεύγονται γιατί συνήθως οδηγούν σε αρνήσεις, συχνά αυτοματοποιημένες

Έμμεσα και υπό καθεστώς έκτακτης ανάγκης. Παρουσιάζεται στο θύμα μια κατάσταση περίπλοκη, όπου εγκύπτουν άμεσες προθεσμίες, έκτακτη απουσία του Διευθυντή, απώλεια συνθηματικού κοκ.

Προσωπική πειθώς. Το θύμα οδηγείται από τον επιτιθέμενο σε μια κατάσταση που του παρουσιάζεται έτσι ώστε:
- Η ενέργειά του, δεν αποτελεί συμμόρφωση, αλλά εθελοντική βοήθεια και προσφορά
- Το θύμα είναι που παίρνει την κρίσιμη απόφαση να βοηθήσει.

Μέτρα για την προστασία από επιθέσεις Κοινωνικής Μηχανικής

- Πολιτική Ασφαλείας
- Κουλτούρα Ασφαλείας στο Προσωπικό
- Καθορισμένος τρόπος συμπεριφοράς
- Καθορισμένη εμφάνιση προσωπικού
- Ζώνες ασφαλείας
- Ελεγχόμενη πρόσβαση
- Εκπαίδευση – καλλιέργεια αυτοματοποιημένης συμπεριφοράς.