SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

TWO-FACTOR-AUTHENTICATION

Όσα πρέπει να γνωρίζω

ΕΛΛΗΝΙΚΟ ΚΕΝΤΡΟ ΑΣΦΑΛΟΥΣ ΔΙΑΔΙΚΤΥΟΥ

help line
saferinternet
210 6007686

Γραμμή Βοηθείας

SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

Ενημέρωση-Επαγρύπνηση

safeLine
www.safeline.gr

Γραμμή παράνομου περιεχομένου

Γιατί οι κωδικοί δεν είναι αρκετοί;

Πριν αναλύσουμε τι είναι το Two-Factor-Authentication 2FA (στα ελληνικά δυο-τρόποι-πιστοποίησης), ας σκεφτούμε γιατί είναι πολύ σημαντικό να κάνουμε ότι περνάει από το χέρι μας για να κρατήσουμε τα δεδομένα μας ασφαλή.

Είναι γεγονός ότι στην ζωή μας καθημερινά συμβαίνουν πολλά μικρά και μεγάλα πράγματα, τα οποία καταγράφονται στις διάφορες συσκευές μας (κινητό, tablet, laptop, έξυπνα ρολόγια, έξυπνα παιχνίδια, έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, κ.τ.λ.). Όλα αυτά τα δεδομένα έχουν γίνει πόλος έλξης για απατεώνες και κακοποιούς. (Κυβερνο)επιθέσεις με ψηφιακά «όπλα» σε κυβερνήσεις, εταιρίες και ιδιώτες έχουν γίνει καθημερινό φαινόμενο. Γι' αυτό το λόγο είναι σήμερα πιο σημαντικό από ποτέ να φροντίζουμε τα δεδομένα μας, αυξάνοντας το επίπεδο της προστασίας που έχουμε στους διάφορους λογαριασμούς μας. Ο παραδοσιακός τρόπος πιστοποίησης ότι έχουμε δικαίωμα πρόσβασης σε ένα λογαριασμό είναι οι κωδικοί. Όμως, επειδή οι άνθρωποι δεν μπορούν να θυμούνται εύκολα τους κωδικούς τους, τείνουν να βάζουν πολύ εύκολους κωδικούς, τους οποίους κάποιος κακόβουλος μπορεί πολύ εύκολα να μαντέψει (π.χ. ημερομηνία γέννησης, "123456", "111111", "password", κ.α.). Επίσης, λόγω του ότι οι άνθρωποι διατηρούν πολλούς λογαριασμούς, τείνουν να βάζουν το ίδιο password σε όλους, και αν μαθευτεί αυτό το ένα password, τότε έχουν πρόσβαση σε όλους τους λογαριασμούς. Έχει αποδειχτεί ότι η αιτία που κάποιες κυβερνο-επιθέσεις επιτυγχάνουν δεν είναι η πολύ υψηλή ευφυΐα των χάκερς, αλλά το ανθρώπινο λάθος (π.χ. πολύ εύκολα passwords, πάτημα πάνω σε links που υπάρχουν σε παραπλανητικά e-mail που παραπέμπουν σε κακόβουλο λογισμικό, κ.τ.λ.).

Η χρήση 2FA

Για τους παραπάνω λόγους εμφανίστηκε η ανάγκη για ακόμα μεγαλύτερη ασφάλεια από αυτή που προσφέρει ένα απλό password. Αυτή η επιπλέον ασφάλεια παρέχεται από το Two-Factor-Authentication (2FA) ή ακόμα και από το Multi-Factor-Authentication (MFA). Τα πολλαπλά επίπεδα πιστοποίησης παρέχουν μεγαλύτερη ακρίβεια στην ερώτηση “Αυτός που προσπαθεί να μπει σε ένα λογαριασμό είναι όντως αυτός που λέει ότι είναι;”. Η διαδικασία αυτής της πιστοποίησης ξεκινάει με την εισαγωγή των κωδικών μας και στην συνέχεια το σύστημα ζητάει άλλο ένα αποδεικτικό (ή περισσότερα ανάλογα με το σύστημα που χρησιμοποιείται) ότι έχουμε δικαίωμα να εισέλθουμε στον λογαριασμό. Το δεύτερο στοιχείο που ζητείται πρέπει να προέρχεται από τις εξής κατηγορίες:

- Κάτι που γνωρίζουμε μόνο εμείς (PIN, μυστική ερώτηση, κ.α).
- Κάτι που κατέχουμε μόνο εμείς (το κινητό μας, μια συσκευή παραγωγής κωδικών, πιστωτική κάρτα).
- Κάτι που είμαστε μόνο εμείς (δακτυλικά αποτυπώματα, φωνητική αναγνώριση, σκανάρισμα ίριδας).

Όταν υπάρχει ένας συνδυασμός των παραπάνω στοιχείων για να μπούμε σε ένα λογαριασμό, ακόμη και να χάσουμε ένα password, ή αν χάσουμε το κινητό μας, δεν μπορεί κάποιος να μπει στους λογαριασμούς μας.

Συνήθεις τύποι 2FA

Υπάρχουν διάφοροι τύποι 2FA που χρησιμοποιούνται σήμερα. Κάποιοι είναι πιο δυνατοί και περίπλοκοι από άλλους, αλλά όλοι είναι πιο ασφαλείς από ένα απλό password.

Μικρές συσκευές παραγωγής έξτρα κωδικών
Είναι μικρές συσκευές που παράγουν κάθε λίγα δευτερόλεπτα ένα νέο κωδικό ο οποίος εμφανίζεται στην οθονούλα της συσκευής. Αυτόν τον τρόπο χρησιμοποιούσαν παλιότερα οι τράπεζες για να δώσουν πρόσβαση στους λογαριασμούς των χρηστών τους διαδικτυακά. Έχουν διάφορα αρνητικά, όπως το έξτρα κόστος της συσκευής και ότι λόγω του μικρού μεγέθους μπορούσε εύκολα να χαθεί.

Μηνύματα SMS
Με αυτόν τον τρόπο, οι χρήστες βάζουν τους κωδικούς τους στο σύστημα και σαν δεύτερο επίπεδο ασφαλείας τους αποστέλεται ένας επιπλέον κωδικός στο κινητό τους μέσω SMS τον οποίον πρέπει να εισάγουν στο σύστημα. Η διάρκεια ζωής του επιπλέον κωδικού που στέλνεται στο κινητό είναι της τάξης των λίγων λεπτών.

Εφαρμογές παραγωγής επιπλέον κωδικών
Με αυτόν τον τρόπο οι χρήστες πρέπει να εγκαταστήσουν μια εφαρμογή παραγωγής επιπλέον κωδικών, είτε στον υπολογιστή τους είτε στο κινητό τους. Μπορούν στη συνέχεια να χρησιμοποιούν αυτή την εφαρμογή και να την συνδέσουν σε όλα τα συστήματα που υποστηρίζουν αυτόν τον τρόπο πιστοποίησης 2FA. Η διαδικασία απαιτεί από τον χρήστη πρώτα να βάλει τον κωδικό του στο σύστημα και μετά να ανοίξει την εφαρμογή παραγωγής επιπλέον κωδικών και να εισάγει τον έξτρα κωδικό που παράγεται από την εφαρμογή. Και εδώ οι έξτρα κωδικοί έχουν διάρκεια ζωής λίγων δευτερολέπτων, γι' αυτό το λόγο αυτός ο τρόπος πιστοποίησης θεωρείται ένας από τους πιο ασφαλείς.

Push ενημερώσεις
Άλλα συστήματα αντί να ζητάνε έξτρα κωδικό, αφήνουν τον χρήστη να μπει με τους απλούς κωδικούς του στο λογαριασμό του και του στέλνουν ένα ενημερωτικό μήνυμα/email κάθε φορά που μπαίνει στον λογαριασμό ή κάνει κάποια ενεργεία. Αυτού του είδους η ασφάλεια είναι περισσότερο παθητική, δηλαδή η εκ των υστέρων ενημέρωση για κάποια ενέργεια (π.χ. είσοδο στο σύστημα ή αγορά με πιστωτική κάρτα, από ότι ενεργητική, δηλαδή αποτροπή της ενέργειας εξ' αρχής, αλλά προσφέρει περισσότερη ευελιξία).

Όλοι θα έπρεπε να χρησιμοποιούμε 2FA όπου μπορούμε

Σύμφωνα με τελευταίες έρευνες, οι κλεμμένοι και αδύναμοι κωδικοί, είναι η κύρια αιτία στη δημιουργία κενών ασφάλειας σε ένα σύστημα. Τα καλά νέα είναι ότι οι μέθοδοι 2FA εξαπλώνονται όλο και περισσότερο και όλο και περισσότεροι οργανισμοί τους υιοθετούν στις διαδικτυακές τους υπηρεσίες. Και εμείς συμφωνούμε, όλοι μας θα έπρεπε όπου είναι δυνατόν να επιλέγουμε 2FA.

Για επιπλέον υποστήριξη...

Ελληνικό Κέντρο Ασφαλούς Διαδικτύου: www.saferinternet4kids.gr

Γραμμή Βοηθείας Helpline: www.help-line.gr

Ανοιχτή Γραμμή Καταγγελιών Παράνομου Περιεχομένου: www.safeline.gr

SaferInternet4Kids.gr

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

INHOPE

ins@fe

Συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση

Διευκόλυνση «Συνδέοντας την Ευρώπη»