Μην το πεις, δείξε το

Πώς η αυτοματοποιημένη εκπαίδευση για την ασφάλεια στον κυβερνοχώρο βοηθά τους εργαζομένους να αποδίδουν χωρίς περιορισμούς

Kaspersky Automated Security Awareness Platform

kaspersky ΕΝΕΡΓΟΠΟΙΗΣΤΕ ΤΟ ΜΕΛΛΟΝ

Ξεκινήστε τη δωρεάν δοκιμαστική έκδοση σήμερα:
k-asap.com/el/

Εισαγωγή

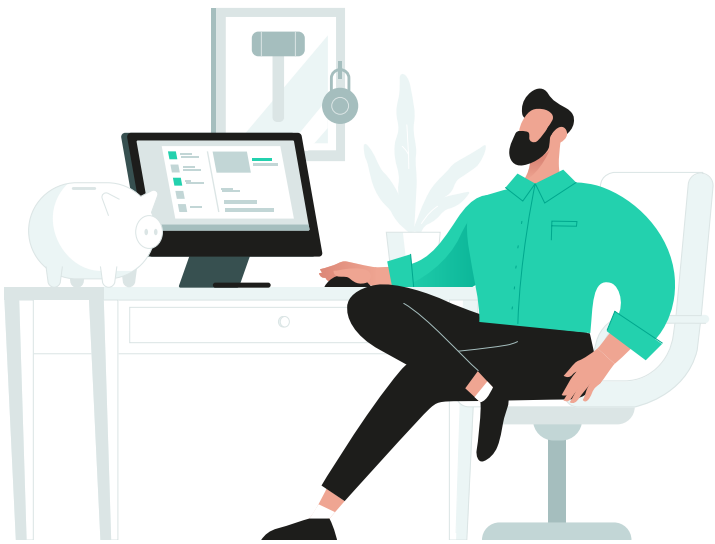
Το 90%[1]
όλων των **περιστατικών στον κυβερνοχώρο** μπορεί να αποδοθεί σε ανθρώπινο σφάλμα

Εάν, όπως πάρα πολλές εταιρείες, έχετε υποφέρει από ένα εσωτερικό περιστατικό ασφάλειας στον κυβερνοχώρο, ίσως έχετε ήδη συνειδητοποιήσει ποιος είναι ο πιο αδύναμος κρίκος της ασφάλειας στον κυβερνοχώρο: ο καλοπροαίρετος, αλλά ανεκπαίδευτος εργαζόμενος. Καθώς τα φίλτρα ηλεκτρονικού "ψαρέματος" και τα firewall έχουν γίνει πιο εξελιγμένα, η εστίαση των εγκληματιών του κυβερνοχώρου έχει στραφεί προς το προσωπικό σας ως πιθανό σημείο εισόδου στα συστήματα IT. Το αποτέλεσμα είναι ότι πάνω από το 90%[1] όλων των περιστατικών στον κυβερνοχώρο μπορεί να αποδοθεί σε ανθρώπινο σφάλμα.

Ζητήματα όπως η απώλεια εμπιστευτικών δεδομένων, ο χρόνος εκτός λειτουργίας και η αστοχία υλικού έχουν σοβαρές οικονομικές συνέπειες. Το μέσο κόστος μιας παραβίασης δεδομένων για τις μικρομεσαίες επιχειρήσεις από ακατάλληλη χρήση IT εσωτερικά ανέρχεται σε 116 χιλ. δολάρια[2], ενώ το μέσο συνολικό κόστος μίας παραβίασης ασφαλείας ανέρχεται σε 3,92 εκ. δολάρια[3]. Εκτιμάται ότι κατά το πρώτο εξάμηνο του 2019, σχεδόν 4.000 παραβιάσεις δεδομένων έθεσαν σε κίνδυνο τα δεδομένα περισσότερων από τέσσερα δισεκατομμύρια χρηστών[4].

Αυτό καταδεικνύει σαφώς την έλλειψη ενημέρωσης των εργαζομένων σχετικά με τις βέλτιστες πρακτικές για την ασφάλεια στον κυβερνοχώρο και ενδεχομένως την έλλειψη κατάλληλης τεχνολογίας εκμάθησης για να εξασφαλιστεί ότι η εκπαίδευση παρέχεται αποτελεσματικά.

Στο παρόν έγγραφο εξετάζονται τα οφέλη της εκπαίδευσης ως μέσου για να εξασφαλίζεται ότι οι εργαζόμενοι μπορούν να χρησιμοποιούν με σιγουριά την τεχνολογία ενός οργανισμού. Συγκεκριμένα, η εκπαίδευση που είναι συνεχής, διαδραστική και ελκυστική – που *δείχνει* αντί να λέει – διασφαλίζει ότι οι εργαζόμενοι έχουν την ελευθερία να αποδίδουν.



1 Ανάλυση των αναφορών παραβίασης δεδομένων που υποβλήθηκαν στο Γραφείο Επιτρόπου Πληροφοριών (Information Commissioner's Office - ICO)

2 Έκθεση Kaspersky – IT security economics του 2019

3 IBM – Έκθεση Cost of a Data Breach, 2019

4 Έκθεση Kaspersky – IT security economics του 2019

Μια πρόκληση για την εργασία στο γραφείο, την εργασία από απόσταση και την εργασία εν κινήσει

Η εξελισσόμενη πολυπλοκότητα του τοπίου του IT σημαίνει ότι οι κυβερνοεπιθέσεις αυξάνονται σε κλίμακα και σοβαρότητα. Οι νέες τεχνολογίες ασφάλειας συμβάλλουν στη μείωση της έκθεσης σε κακόβουλες απειλές, αλλά οι συμπεριφορές μας τόσο ως καταναλωτές τεχνολογίας όσο και ως εργαζόμενοι στο εργατικό δυναμικό έχουν πλέον τον μεγαλύτερο αντίκτυπο στην ασφάλεια του οργανισμού.

Είμαστε όλο και πιο συνδεδεμένοι, πιο κινητοί, μεταφέρουμε περισσότερες προσωπικές συσκευές και χρησιμοποιούμε πιο πολλές δωρεάν και δημοφιλείς υπηρεσίες στην καθημερινή μας ζωή. Οι φορητές συσκευές αποτελούν πλέον αναπόσπαστο μέρος των επιχειρηματικών διαδικασιών του 75% των επιχειρήσεων, ωστόσο μόνο το 17% των εργοδοτών προτιμούν να παρέχουν εταιρικά τηλέφωνα σε ολόκληρο το προσωπικό τους[1]. Οι υπόλοιποι επιτρέπουν τη χρήση προσωπικών συσκευών στην εργασία σε κάποιο βαθμό, γεγονός που ενέχει μεγαλύτερο κίνδυνο.

Η συνεχής αύξηση της εργασίας από απόσταση αλλάζει επίσης τη δυναμική. Ενώ οι εταιρείες είναι σε θέση να προστατεύουν πλήρως τα δίκτυα και τις συσκευές στον χώρο εργασίας, τα ίδια εταιρικά πρότυπα δεν παρέχονται στο σπίτι. Σε πρόσφατη έρευνα για την εργασία από το σπίτι[2], το 47% των ατόμων που ερωτήθηκαν δήλωσαν ότι αφιέρωσαν περισσότερο χρόνο στην παρακολούθηση βίντεο, με περίπου έναν στους δύο (48%) να το κάνουν αυτό σε συσκευές που χρησιμοποιούν για την εργασία τους. Το πιο περίεργο είναι ότι οι μισοί (51%) εργαζόμενοι που παρακολουθούν περιεχόμενο ενηλίκων παραδέχονται ότι το παρακολουθούν στις συσκευές εργασίας τους, με τη σχετική απειλή κακόβουλου λογισμικού από αυτές τις τοποθεσίες. Δεν βοηθά το γεγονός ότι το 73% των εργαζομένων δεν έχουν λάβει εκπαίδευση ενημέρωσης σε θέματα ασφάλειας IT από τον εργοδότη τους από τη στιγμή της μετάβασής τους στην εργασία από το σπίτι.

«Οι εγκληματίες του κυβερνοχώρου μετατοπίζουν την εστίαση με στόχο τους εργαζόμενους από απόσταση με νέες απειλές στον κυβερνοχώρο και νέες μορφές χειραγώγησης»

Οι εγκληματίες του κυβερνοχώρου μετατοπίζουν την εστίαση στοχεύοντας τους εργαζόμενους από απόσταση με νέες απειλές στον κυβερνοχώρο και νέες μορφές χειραγώγησης, επομένως η ενίσχυση της ενημέρωσης σχετικά με τη βασική ασφαλή συμπεριφορά είναι πιο σημαντική από ποτέ. Η εκπαίδευση πρέπει επίσης να εξελίσσεται ώστε να είναι πιο αξιόλογη και αποτελεσματική, διασφαλίζοντας ότι οι εργαζόμενοι μπορούν να αντιμετωπίζουν διαφορετικές απειλές, από εύκολες μαζικές επιθέσεις έως πιο εξελιγμένες επιθέσεις.

1 Μελέτη του Oxford Economics για τη Samsung, 2018

2 Kaspersky – “How Covid-19 changed the way people work”, 2020

Γιατί ξεχνιέται τόσο πολλή εκπαίδευση

Τα περιστατικά ασφάλειας στον κυβερνοχώρο μπορούν να μειωθούν σημαντικά με την αποτελεσματική διαδραστική εκπαίδευση μέσω υπολογιστή

Για να γίνει μια ριζική αλλαγή στον τρόπο με τον οποίο οι εργαζόμενοι αποκτούν μεγαλύτερη επίγνωση της ασφάλειας στον κυβερνοχώρο, η εκπαίδευση πρέπει να είναι πιο ελκυστική προκειμένου να ενσταλάζει νέες γνώσεις. Η εκμάθηση που βασίζεται σε μεγάλο βαθμό στο χαρτί ή εξαρτάται από την παρακολούθηση βίντεο δεν αποτελεί αποτελεσματικό τρόπο για την προώθηση της μάθησης, δεδομένου ότι πολλοί εργαζόμενοι βρίσκουν το μέσο βαρετό και το περιεχόμενο ξεχνιέται.

Για να μην ξεχαστεί, η εκπαίδευση πρέπει να αντιμάχεται την «καμπύλη λήθης» του Ebbinghaus, όπου η διατήρηση της μνήμης μειώνεται με την πάροδο του χρόνου. Οι μαθησιακές μεθοδολογίες πρέπει να βασίζονται στην ανθρώπινη μνήμη και στην ψυχολογία της συμπεριφοράς και να αναγνωρίζουν την τεράστια σημασία της ενσυναίσθησης στην εκπαίδευση και την κατάρτιση. Ακολουθούν δύο παραδείγματα όπου η παραδοσιακή εκμάθηση αποτυγχάνει από αυτήν την άποψη. Πρώτον, εκπαιδευτικό περιεχόμενο που δεν σχετίζεται με τις πραγματικές καταστάσεις που αντιμετωπίζουν οι άνθρωποι στην εργασία. Δεύτερον, μη ευέλικτα μαθήματα που δεν είναι οπτικά ελκυστικά και διαδραστικά και έτσι μειώνουν τα ποσοστά συμμετοχής και δεν αλλάζουν σημαντικά τη συμπεριφορά όσον αφορά την ασφάλεια στον κυβερνοχώρο.

Τα εκπαιδευτικά μαθήματα κατάρτισης που δεν είναι ελκυστικά για τους εργαζόμενους ξεχνιούνται εξίσου γρήγορα με τις δεξιότητες που υποτίθεται ότι διδάσκουν. Για παράδειγμα, σε μία επιχείρηση, ο μέσος ρυθμός κλικ σε email ηλεκτρονικού "ψαρέματος" ήταν περίπου 40% μεταξύ του προσωπικού. Αμέσως μετά την εκπαίδευση το ποσοστό αυτό μειώθηκε, ωστόσο επανήλθε στο 40% μέσα σε λίγους μήνες[1].

Αντίθετα, η επανειλημμένη ενίσχυση με τη ηλεκτρονική διαδραστική εκπαίδευση, όπως το Kaspersky Automated Security Awareness Platform (ASAP), περιλαμβάνει τεστ γνώσεων και υψηλά επίπεδα αλληλεπίδρασης, καθιστώντας τη μάθηση αξιομνημόνευτη και συμβάλλοντας στη δημιουργία ισχυρών, μακροχρόνιων δεξιοτήτων για την ασφάλεια στον κυβερνοχώρο. Είναι αποτελεσματική διότι παρέχει γνώσεις και καλλιεργεί καλύτερα πρότυπα και συνήθειες ασφαλούς συμπεριφοράς στον κυβερνοχώρο.

1 Kaspersky – “IT security economics in 2019”, σχόλια συμμετέχοντος

Μην το πεις, δείξε το: Ο ρόλος της αλληλεπίδρασης και σενάρια ασφάλειας στον κυβερνοχώρο

«Δυσκολευόμασταν να προσφέρουμε εκπαίδευση που πραγματικά είχε αποτέλεσμα σε αίθουσες διδασκαλίας. Η αυτοματοποίηση της εκπαίδευσης με την Kaspersky είχε πολύ μεγαλύτερη επιτυχία και μετά από 6 μήνες χρήσης αναφέρουμε πολύ λιγότερα περιστατικά στον κυβερνοχώρο.»

Διευθυντής ανθρώπινου δυναμικού στον τομέα της μεταποίησης

Αντί για την ανάγνωση ή την ακρόαση της θεωρίας της ασφάλειας στον κυβερνοχώρο, η εκπαίδευση μπορεί να γίνει πιο συναρπαστική και ελκυστική μέσω πολυτροπικού περιεχομένου, όπου διάφορα εκπαιδευτικά στοιχεία αλληλοσυμπληρώνονται για την ανάπτυξη δεξιοτήτων, όπως, για παράδειγμα, διαδραστικά μαθήματα, τεστ, ενίσχυση και προσομοιωμένες επιθέσεις.

Τα ρεαλιστικά σενάρια για την ασφάλεια στον κυβερνοχώρο και οι προσομοιωμένες επιθέσεις αποτελούν σημαντικό στοιχείο μιας προσέγγισης «μην το πεις, δείξε το». Βοηθούν τους εργαζόμενους να είναι σε εγρήγορση και να ενεργούν με βάση την κατανόησή τους. Αυτό ενισχύει τη συμπεριφορά ασφάλειας στον κυβερνοχώρο όταν πρέπει να ληφθούν αποφάσεις κατά τη διάρκεια μιας πραγματικής επίθεσης.

Όταν το πολυτροπικό περιεχόμενο υποστηρίζεται από μια σαφή δομή προγράμματος, η εκπαίδευση θα είναι εύκολα κατανοητή, λογική και ισορροπημένη. Κατά τη διάρκεια του προγράμματος θα πρέπει να υπάρχει ένα στοιχείο παρακίνησης για την παροχή κινήτρων και η εκπαίδευση δεν θα πρέπει ποτέ να είναι «μίας κατεύθυνσης». Η συνεχής και σταδιακή μάθηση – με υπενθυμίσεις για προηγούμενα θέματα και ενίσχυση των συνηθειών – είναι ο πιο αποτελεσματικός τρόπος για να διασφαλίζεται η συμμετοχή των εργαζομένων και η διατήρηση των πληροφοριών.

Συμβάλλει επίσης στη δημιουργία του εκπαιδευτικού περιεχομένου από έναν οργανισμό που επικεντρώνεται στην ασφάλεια στον κυβερνοχώρο με ειδικευμένο προσωπικό στον τομέα της ασφάλειας, αντί στην ίδια την εκπαίδευση. Στην περίπτωση της Kaspersky, η εταιρεία διαθέτει πάνω από 20 χρόνια εμπειρίας στον τομέα της ασφάλειας στον κυβερνοχώρο και επομένως γνωρίζει τις δεξιότητες που θα πρέπει να αναπτύξουν οι εργαζόμενοι προκειμένου να συμπεριφέρονται με ασφάλεια και να προστατεύουν την εταιρεία. Αυτές οι δεξιότητες ενσωματώνονται απευθείας στο περιεχόμενο της εκπαίδευσης, διαιρεμένες ανά θέματα και επίπεδα.

Η απλότητα παρέχεται μέσω αυτοματοποίησης

Όπως αναφέρθηκε, για να ενισχυθούν τα νέα πρότυπα συμπεριφοράς, η εκπαίδευση ενημέρωσης για την ασφάλεια θα πρέπει να είναι συνεχής, με τακτικές επαναληπτικές συνεδρίες, για να δίνεται έμφαση στα αποτελέσματα εκμάθησης από προηγούμενα μαθήματα. Η μη αυτόματη ανάθεση όλου αυτού του υλικού θα αποτελούσε πρόκληση για πολλούς διαχειριστές – ιδίως σε μικρότερες επιχειρήσεις με περιορισμένους πόρους – ενώ η αυτοματοποίηση το κάνει χωρίς κόπο για εξοικονόμηση χρόνου.

Η αυτοματοποίηση μπορεί επίσης να εξαλείψει την πολυπλοκότητα των προγραμμάτων και να επιτρέψει την τελειοποίηση, τη διαχείριση και την παροχή εκπαίδευσης σε ένα ευρύ φάσμα εργαζομένων με διαφορετικά επίπεδα μαθησιακών απαιτήσεων για την ασφάλεια στον κυβερνοχώρο. Η εκπαίδευση χωρίζεται σε μικρότερα μαθήματα βήμα προς βήμα, τα οποία επιτρέπουν την ευκολότερη παρακολούθηση της προόδου προς την επίτευξη συγκεκριμένων εκπαιδευτικών στόχων. Αυτό ξεπερνά τους περιορισμούς της παραδοσιακής εκπαίδευσης στην αίθουσα, η οποία δεν μπορεί να φτάσει σε μεγάλους αριθμούς και συχνά παρέχει ελάχιστες αποδείξεις ότι πληρούνται οι απαιτήσεις.

Αντίθετα, η ηλεκτρονική διαδραστική εκπαίδευση μειώνει τον χρόνο διαχείρισης, δεν θυσιάζει το βάθος της εκπαίδευσης. Με το Kaspersky ASAP είναι δυνατή η διδασκαλία περισσότερων από 300 πρακτικών δεξιοτήτων, με αυτόματα εκπαιδευτικά προγράμματα για κάθε ομάδα εργαζομένων.

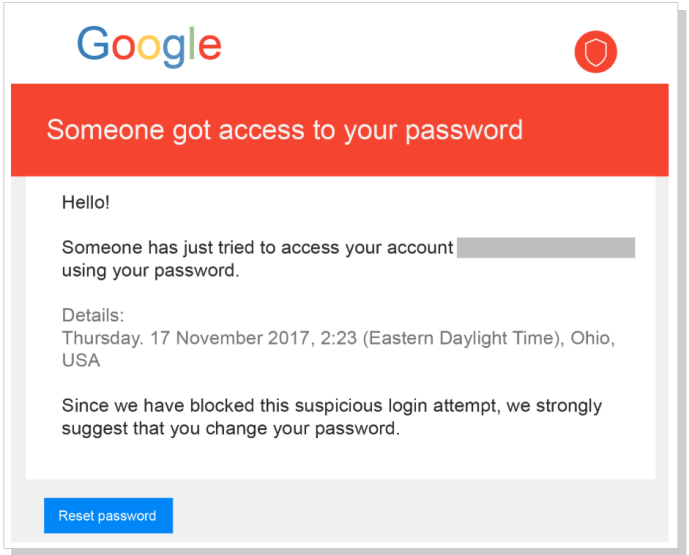
Δείξτε τον δρόμο: Ένα παράδειγμα εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο

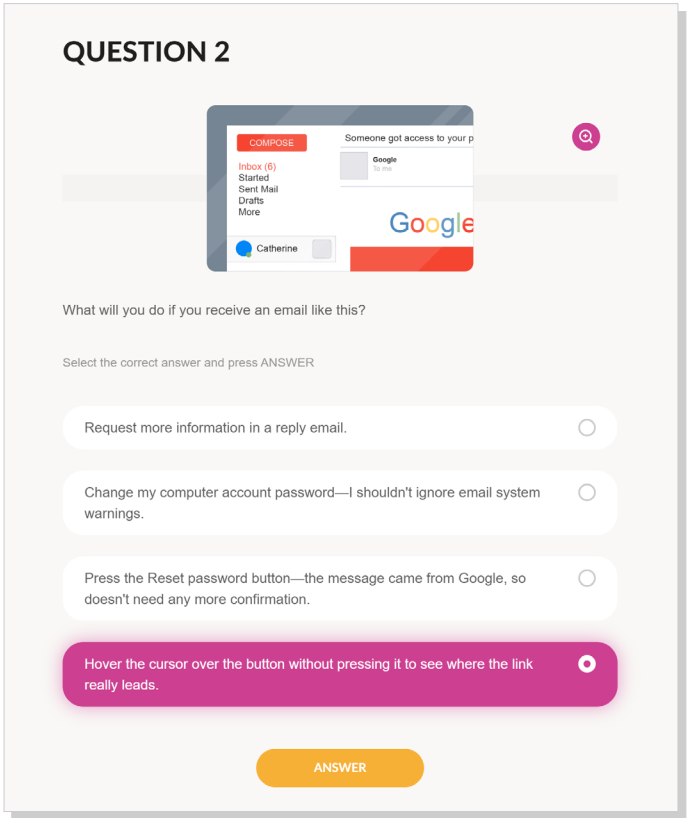
Προσομοιωμένες επιθέσεις ηλεκτρονικού «ψαρέματος»

Υπάρχουν πάρα πολλοί άνθρωποι που πιστεύουν ότι δεν θα μπορούσε να τους συμβεί μια επίθεση ηλεκτρονικού "ψαρέματος". Έτσι, με το Kaspersky ASAP, μετά από διαδραστικά μαθήματα, τεστ και ενίσχυση της εκμάθησης, ξεδιπλώνεται ένα σενάριο από την πραγματική ζωή και ο εργαζόμενος βρίσκεται στο επίκεντρο της διαδικασίας.

Αυτό το εκπαιδευτικό παράδειγμα προκαλεί τον εργαζόμενο να δει εάν είναι αρκετά εξοικειωμένος για να αναγνωρίσει τα σημάδια ενός πλαστογραφημένου email. Ποια είναι τα σημάδια κινδύνου; Πώς μπορεί να ελέγξει την αυθεντικότητα του ονόματος και της διεύθυνσης του αποστολέα; Τι πρέπει να κάνει εάν υποψιάζεται ηλεκτρονικό "ψάρεμα";

Το περιεχόμενο είναι σκόπιμα σύντομο, ενδιαφέρον, θέτει προκλήσεις και είναι αξιοσημείωτο. Επιλύοντας το πρόβλημα, ο εργαζόμενος αποκτά μια αίσθηση επιτυχίας – «μια νίκη κάθε μέρα» – και οι δεξιότητες που έχουν αποκτηθεί μπορούν να αξιοποιηθούν αμέσως μετά από ένα μόνο μάθημα, για την προστασία της εταιρείας.





Συμπέρασμα

Οι υπεύθυνοι λήψης αποφάσεων στον τομέα του IT και της ασφάλειας αρχίζουν να συνειδητοποιούν τη σημασία της εκπαίδευσης των εργαζομένων τους στα θέματα ασφάλειας. Στη συνέχεια, πρέπει να επιλέξουν έναν προμηθευτή και μια εκπαιδευτική λύση που θα προσφέρει μακροπρόθεσμα αποτελέσματα. Η εκπαίδευση πρέπει να χρησιμοποιεί καλύτερες αρχές εκμάθησης και διαδραστικό περιεχόμενο που να προωθεί συμπεριφορά με γνώμονα την ασφάλεια στις πραγματικές καταστάσεις, ενσταλάζοντας νέες γνώσεις και καταστέλλονται την «καμπύλη λήθης».

Η κατάλληλη κατάρτιση θα παρέχει οφέλη πέρα από τα οικονομικά, συμπεριλαμβανομένης της βελτίωσης του ηθικού και της σιγουριάς των εργαζομένων, καθώς και βελτιωμένης εργασιακής κουλτούρας. Χρησιμοποιώντας την εκπαίδευση *μην το πεις, δείξε το*, οι εργαζόμενοι μπορούν πραγματικά να έχουν την ελευθερία να αποδίδουν χωρίς περιορισμούς.

Δωρεάν δοκιμαστική έκδοση Kaspersky ASAP: k-asap.com/el/
Νέα για την ασφάλεια IT: business.kaspersky.com
Ενημέρωση για την ασφάλεια της Kaspersky: kaspersky.com/awareness

kaspersky ΕΝΕΡΓΟΠΟΙΗΣΤΕ ΤΟ ΜΕΛΛΟΝ

www.kaspersky.com