

مقياس الوعي بالسلوك الأمني

Oct 9, 2026 · @Yusef

دليل المقياس

يقيس هذا المقياس ما يفعله الموظف حين يواجه موقفاً أمنياً، لا ما يحفظه من تعريفات. بُني على محتوى برنامج «أمن المعلومات السلوكي» (3 أيام 18٠ ساعة)، ويُطبَّق قبلياً وبعدياً لقياس أثر البرنامج على منسوبي الجهة.

الفكرة الحاكمة: معرفة القاعدة لا تعني تطبيقها (فجوة المعرفة والتطبيق: أعرف ← أقتنع ← أقدر ← أفعل). لذلك يجمع المقياس بين محاكاة القرار، واكتشاف المؤشرات، وتحليل حالات حقيقية، وقياس القنوات، ثم يتحقق من النتائج بتجارب ميدانية على السلوك الفعلي.

الإطار النظري

النموذج (من البرنامج)	ما يقيسه في المقياس
النظام الأول والثاني والتحيزات المعرفية	القرار تحت الإلحاح والسلطة والألفة وتحيز التفاؤل
هندسة الحيل الاجتماعية (الخوف، الطمع، السلطة، الفضول)	اكتشاف المحفز النفسي وأسلوب الهجوم (تصيد، ذريعة، طُعم، مقايضة)
TPB) نظرية السلوك المخطط	الاتجاه، والمعايير الاجتماعية، والتحكم السلوكي المدرك
HBM) نموذج الاعتقاد الصحي	القابلية والخطورة المدركة، والفوائد والعوائق، والكفاءة الذاتية
COM-B نموذج	تفسير سبب الضعف: قدرة، أم فرصة، أم دافع
أنماط المستخدمين الأربعة	تصنيف المستجيب: متعاون، متجاهل، مقاوم، متهور
بيئة الإبلاغ بلا لوم	سلوك ما بعد الخطأ وسرعة الإبلاغ

الأبعاد الستة

الرمز	البعد	أمثلة على السلوك المقاس
1د	كشف الهندسة الاجتماعية والتصيد	التصيد بالبريد والهاتف والرسائل، الذريعة، الطُعم، إرهاب التحقق الثنائي
2د	القرار تحت الضغط والتحيزات المعرفية	طلبات باسم القيادة، الفواتير المألوفة، تأجيل التحديثات

الرمز	البعد	أمثلة على السلوك المقاس
3د	الامتثال للسياسات في الممارسة اليومية	التتبع عند الأبواب، المكتب النظيف، وسائل التواصل، الوسائط القابلة للإزالة
4د	الاستجابة للحوادث والإبلاغ	الدقائق الأولى بعد النقر، الفدية، التعامل مع خطأ زميل
5د	بيئات العمل الحديثة والذكاء الاصطناعي	تقنية الظل، العمل عن بعد، الأجهزة الشخصية، التزييف العميق
6د	القناعات والثقافة الأمنية	إدراك الخطر، الكفاءة الذاتية، سلوك القادة والزملاء

مكونات المقياس

الجزء	النوع	البند	الدرجة	الزمن التقريبي
الأول	مواقف الحكم السلوكي (محاكاة قرار)	موقفاً 15	45	دقيقة 20
الثاني	محاكاة اكتشاف المؤشرات	محاكيات 3	30	دقيقة 15
الثالث	تحليل حالات حقيقية	حالات 3	24	دقيقة 20
الرابع	السلوك المعلن والقناعات (ليكرت)	بنداً 2 + للصدق 24	120	دقائق 10
الخامس	تجارب ميدانية على السلوك الفعلي	تجارب 5	مؤشر مستقل	على مدى الربع

الأجزاء من الأول إلى الرابع تُطبَّق في جلسة واحدة (نحو 65 دقيقة). للتطبيق القبلي السريع يكفي الأول والثاني والرابع (نحو 45 دقيقة).

تعليمات المستجيب

- اقرأ كل موقف كأنه يحدث لك الآن في عملك، واختر ما ستفعله فعلاً، لا ما تظن أنه الإجابة المطلوبة.
- لا توجد عقوبة على أي إجابة؛ النتائج تُستخدم لتصميم التوعية لا لتقييمك وظيفياً.
- يُستبدل بنطاق الجهة الفعلي عند energy.gov.sa لأغراض التمرين، النطاق الرسمي لبريد الجهة هو. (التطبيق).

الجزء الأول: مواقف الحكم السلوكي

خمسة عشر موقفاً من بيئة العمل، لكل موقف أربعة تصرفات محتملة. اختر التصرف الذي ستقوم به فعلاً. كل الخيارات تبدو معقولة، لكنها تختلف في درجة الأمان (الأوزان في مفتاح التصحيح).

البعد الأول: كشف الهندسة الاجتماعية

الموقف 1. الساعة 11 ليلاً تصلك على جوالك تسعة إشعارات متتالية تطلب الموافقة على تسجيل دخول لحسابك في الجهة، ولم تطلبها. بعد دقائق يتصل بك رقم يعرّف نفسه بـ«الدعم الفني»، ويذكر اسمك وإدارتك، ويقول إن الإشعارات ستوقف إذا وافقت على آخر طلب. ماذا تفعل؟

- (أ) توافق على الطلب الأخير لإيقاف الإزعاج، فالمتصل يعرف بياناتك.
- (ب) ترفض الطلبات وتنتهي المكالمة، وتساءل زملاءك صباحاً إن حدث معهم الشيء نفسه.
- (ج) ترفض الطلبات وتغيّر كلمة المرور بنفسك دون إبلاغ أحد.
- (د) ترفض جميع الطلبات، وتنتهي المكالمة، وتبلغ فريق الأمن فوراً عبر القناة المعتمدة.

الموقف 2. يزورك شخص ببطاقة باسم «هيئة رقابية»، ويقول إنه يجري تدقيقاً عاجلاً بتكليف من الوكيل، أحضرها معه USB ويطلب نسخ قائمة صلاحيات المستخدمين على نظام التحكم بالمحطة إلى ذاكرة.

- (أ) تعتذر بلطف، وتحقق من التكليف عبر مكتب الوكيل أو إدارة الأمن برقم من الدليل الرسمي، ولا تسلم شيئاً إلا عبر القناة الرسمية.
- (ب) تطلب خطاب التكليف، فإن أبرزه نسخت له القائمة على ذاكرته.
- (ج) تسلمه القائمة، فالتدقيق إلزامي والطلب باسم الوكيل.
- (د) ترفض طلبه وتطلب منه المغادرة دون أن تبلغ أحداً.

«عليها ملصق «رواتب ومكافآت الإدارة USB 2026 الموقف 3. في مواقف السيارات تجد ذاكرة

- (أ) توصلها بجهاز العمل لمعرفة صاحبها وإعادتها إليه.
- (ب) تسلمها لمكتب الاستقبال ضمن المفقودات.
- (ج) تسلمها لفريق الأمن السيبراني دون توصيلها، وتخبرهم بمكان العثور عليها.
- (د) تتلفها وترميها حتى لا يستخدمها أحد.

البعد الثاني: القرار تحت الضغط والتحيزات

الموقف 4. قبل نهاية الدوام بعشر دقائق يصلك بريد يحمل اسم الوكيل المساعد: «أنا في اجتماع مغلق ولا أستطيع الرد على الهاتف. أرسل لي تقرير الطاقة الإنتاجية للمحطات حالاً على هذا البريد، الوزير ينتظره

- (أ) ترسله فوراً، فالتأخير قد يحرّك أمام القيادة.
- (ب) تتأكد أن عنوان البريد ينتهي بنطاق الجهة ثم ترسله.
- (ج) تتجاهل البريد ولا ترسل شيئاً.
- (د) تتحقق عبر قناة ثانية معروفة (هاتف مكتبه من الدليل أو مدير مكتبه) قبل الإرسال، وتبلغ الأمن إن لم يتأكد الطلب.

الموقف 5. تصلك فاتورة من مورّد تتعامل معه منذ سنوات، بال قالب المعتاد نفسه، مع ملاحظة: «نرجو التحويل إلى حسابنا البنكي الجديد بسبب تحديث إجراءاتنا».

- (أ) تتصل بالمورد على الرقم المسجّل لديكم مسبقاً، وتتبع إجراء التحقق المزدوج لتغيير الحساب، وتنبّه الإدارة المالية.
- (ب) تتصل بالمورد على الرقم المذكور في الفاتورة للتأكد.

- (ج) تعتمد، فكل شيء مطابق للمعتاد.
- (د) ترد على البريد وتطلب خطاباً رسمياً مختوماً بالحساب الجديد.

الموقف 6. يظهر على جهاز العمل تنبيه بتحديث أمني حرج يتطلب إعادة التشغيل، وأمامك عرض يجب تسليمه بعد ساعتين. أُجّلت هذا التحديث أربع مرات هذا الأسبوع ولم يحدث شيء.

- (أ) تؤجله مرة أخرى، فلم يحدث شيء في المرات السابقة.
- (ب) تحفظ عملك وتعيد التشغيل في أقرب فاصل خلال اليوم نفسه.
- (ج) تؤجله إلى نهاية الأسبوع حين يخف الضغط.
- (د) تطلب من الدعم الفني إيقاف هذه التنبيهات لأنها تعطلك.

البعد الثالث: الامتثال في الممارسة اليومية

الموقف 7. تدخل غرفة التحكم المقيدة ببطاقتك، فيلحق بك رجل يحمل صناديق ويرتدي سترة شركة «صيانة، ويقول مبتسماً: «ممكن تمسك الباب؟ يدي مشغولة والبطاقة في جيبى».

- (أ) تمسك الباب له، فالمساعدة من الذوق.
- (ب) تمسك الباب وتراقبه حتى ينتهي من عمله.
- (ج) تعتذر بلطف، وتعرض أن تحمل عنه الصناديق ريثما يمرر بطاقتك، أو توجّه لمكتب الأمن.
- (د) تسأله عن اسم شركته، ثم تدخله.

الموقف 8. تطيع تقرير «مخطط الشبكة الصناعية للمحطة» على الطابعة المشتركة، فتُسندعى إلى اجتماع طارئ فوراً.

- (أ) تذهب للاجتماع وتأخذ التقرير بعد عودتك.
- (ب) تطلب من زميل أن يأخذه ويضعه على مكتبك.
- (ج) تقفل جهازك فقط وتذهب.
- (د) تقفل جهازك، وتأخذ المطبوع معك أو تلغي الطابعة قبل أن تذهب.

الموقف 9. نشر زميلك صورة احتفالية في غرفة التحكم بمناسبة رقم قياسي، وتظهر خلفه شاشة بأسماء الأنظمة وجزء من لوحة البيانات، الصورة حصدت تفاعلاً كبيراً.

- (أ) تتواصل معه على انفراد، وتطلب حذفها موضحاً ما تكشفه الخلفية، وتبلغ الأمن إن تضمنت بيانات حساسة.
- (ب) تتجاهل الأمر، فهو حسابه الشخصي.
- (ج) تعيد نشرها فخراً بالإنجاز.
- (د) تكتب تعليقاً علنياً تنبهه فيه إلى خطورة الصورة.

البعد الرابع: الاستجابة والإبلاغ

الموقف 10. نقرت على رابط في بريد يبدو من الموارد البشرية بعنوان «تحديث بيانات الراتب»، وأدخلت اسم المستخدم وكلمة المرور، ثم لاحظت أن عنوان الصفحة غريب.

- (أ) تغلق الصفحة وتغيّر كلمة المرور، ولا تخبر أحداً حتى لا تُحاسَب.

- (ب) تحذف البريد كي لا ينقر عليه غيرك.
- (ج) تبليغ فريق الأمن فوراً، وتغيير كلمة المرور، وتحتفظ بالبريد، وتدوّن ما حدث ومتى.
- (د) تنتظر لترى هل سيحدث شيء غير طبيعي في حسابك.

الموقف 11. أثناء العمل تتغير أسماء الملفات في المجلد المشترك أمامك، ثم تظهر رسالة تطلب فدية.

- (أ) تطفئ الجهاز فوراً.
- (ب) تفصل الجهاز عن الشبكة دون إطفائه، وتبليغ الأمن فوراً، وتصوّر الرسالة أو تدوّنوها.
- (ج) تحاول استعادة الملفات من النسخة السابقة بنفسك أولاً.
- (د) تبليغ مديرك المباشر بعد انتهاء اجتماعك الحالي.

الموقف 12. أنت مدير إدارة، أبلغك أحد موظفيك أنه أرسل بالخطأ قبل ساعة ملفاً يحوي بيانات موظفين إلى جهة خارجية.

- (أ) توبّخه أمام الفريق ليكون درساً للجميع.
- (ب) تشكره على سرعة الإبلاغ، وتصعد فوراً لفريق الأمن للاحتواء، ثم تراجع الحادثة بسؤال «كيف حدث؟» لا «من أخطأ؟».
- (ج) تطلب منه مراسلة الجهة الخارجية لحذف الملف، وتغلق الموضوع دون تصعيد.
- (د) ترفع الأمر للموارد البشرية لاتخاذ إجراء تأديبي.

البعد الخامس: بيئات العمل الحديثة

خلال 15 دقيقة، والأداة المعتمدة بطيئة PDF **الموقف 13.** عليك تحويل ملف عقود كبير إلى

- (أ) تستخدم الأداة المعتمدة ولو تأخرت قليلاً، وتبليغ تقنية المعلومات ببطلتها ليؤقّر بديل.
- (ب) ترسله إلى بريدك الشخصي لتحوّله على جهازك.
- (ج) ترفعه إلى موقع تحويل مجاني على الإنترنت.
- (د) تطلب من زميل لديه برنامج مثبت على جهازه الشخصي أن يحوّله لك.

الموقف 14. أنت في صالة المطار وعليك اعتماد طلب عاجل في النظام الداخلي. شبكة الصالة المفتوحة متاحة، ولديك باقة بيانات في جوالك.

- (أ) تتصل بشبكة الصالة وتعتمد الطلب بسرعة.
- (ب) الجهة VPN تتصل بشبكة الصالة ثم تفعل.
- (ج) الجهة، وتجلس بحيث لا تُرى شاشتك VPN (ج) تستخدم نقطة اتصال جوالك مع.
- (د) تؤجل الاعتماد حتى تصل المكتب ولو تأخر العمل.

الموقف 15. يتصل بك رقم غير محفوظ بصوت يطابق تماماً صوت مديرك العام، ويطلب بلهجة مستعجلة «تعطيل التحقق الثنائي لحساب أحد المقاولين» لأن الاجتماع مع الوزير بعد دقائق.

- (أ) تنقذ الطلب، فالصوت صوته بلا شك.
- (ب) تخبره أنك ستعاود الاتصال على رقمه المعروف، ولا تنقذ إلا بعد التأكيد وعبر إجراء الطلب الرسمي، وتبليغ الأمن إن لم يتأكد.
- (ج) تطلب منه إرسال الطلب بالبريد ثم تنقذ.

- (د) تسأله سؤالاً شخصياً لا يعرفه غيره، فإن أجاب نفّذت

الجزء الثاني: محاكاة اكتشاف المؤشرات

أمامك ثلاث رسائل مُحاكاة كما تصل فعلاً. صنف كل عنصر تحتها في أحد ثلاثة خيارات، ثم اختر الإجراء الأنسب. لكل محاكاة 10 درجات: 8 للتصنيف و2 للإجراء

خيارات التصنيف: (خ) مؤشر خطر · (م) عنصر محايد لا يُثبت السلامة ولا الخطر · (س) دليل على سلامة الرسالة

المحاكاة الأولى: بريد إلكتروني

<it-support@energy-gov-sa.com> من: إدارة تقنية المعلومات
إلى: جميع المنسوبين
الموضوع: إجراء عاجل - سيتم تعليق حسابك خلال 60 دقيقة

[شعار الجهة وألوانها الرسمية]

،عزيزي الموظف،

،رصدت أنظمتنا محاولات دخول غير اعتيادية إلى حسابك. حفاظاً على أمن بياناتك،
يرجى التحقق من هويتك خلال 60 دقيقة بإدخال اسم المستخدم وكلمة المرور
،ورمز التحقق المرسل إلى جوالك، وإلا سيتم تعليق الحساب تلقائياً

[تحقق من حسابي]

(http://energy-verify.account-secure.co/login :عند تمرير المؤشر يظهر)

،مع التحية،

فريق الدعم الفني - تحويل 4455

#	العنصر	التصنيف (خ / م / س)
1	energy-gov-sa.com عنوان المرسل	
2	«التحية العامة» عزيزي الموظف	
3	مهلة 60 دقيقة والتهديد بالتعليق	
4	طلب رمز التحقق المرسل إلى الجوال	
5	الرابط الظاهر عند تمرير المؤشر	
6	الشعار والألوان الرسمية	
7	رقم التحويلة الداخلية في التوقيع	
8	اللغة سليمة وخالية من الأخطاء	

الإجراء الأنسب:

- (أ) أحذف الرسالة وأكمل عملي
- (ب) أتصل على التحويلة 4455 للتأكد
- (ج) أبلغ عنها عبر زر الإبلاغ أو القناة المعتمدة دون النقر على أي رابط
- (د) أعيد توجيهها لزملائي لتحذيرهم

المحاكاة الثانية: رسالة نصية على جوالك الشخصي

المرسل : SHIP-Express

عزيزي العميل، شحنة قطع الغيار رقم 88412 الخاصة بمحطتك متوقفة في الجمارك لنقص رسوم قدرها 12.50 ريال. يرجى السداد خلال 24 ساعة
 bit.ly/3xR-pay :لتجنب إعادة الشحنة

ملاحظة: إدارتك تنتظر فعلاً شحنة قطع غيار هذا الأسبوع.

#	العنصر	التصنيف (خ / م / س)
1	الرابط المختصر	
2	المبلغ الزهيد (12.50 ريال)	
3	مهلة 24 ساعة	
4	وصول رسالة عن شحنة عمل إلى جوالك الشخصي	
5	ذكر رقم شحنة محدد	
6	اسم المرسل يشبه شركة شحن معروفة	

#	العنصر	التصنيف (خ / م / س)
7	«التحية العامة» عزيزي العميل	
8	توافق الرسالة مع شحنة تنتظرها فعلاً	

الإجراء الأنسب:

- (أ) أسدد المبلغ، فهو زهيد ولا يستحق تعطيل الشحنة
- (ب) أفتح الرابط لأرى التفاصيل دون إدخال بيانات
- (ج) أتجاهل الرسالة
- (د) لا أفتح الرابط، وأتحقق من حالة الشحنة عبر إدارة المشتريات أو موقع الشركة الرسمي، وأبلغ الأمن عن الرسالة

المحاكاة الثالثة: نص مكالمة هاتفية

المتصل: السلام عليكم، معك فيصل من الدعم الفني. أستاذ عبدالله، أنت في إدارة التشغيل صح؟
الموظف: نعم، تفضل.
المتصل: عندنا الليلة نقل لنظام البريد، وحسابك طلع فيه خطأ مزامنة. ما أبغى بريدك
. يتعطل بكرة الصبح قدام المدير
المتصل: بيوصلك الحين رمز على جوالك، اقرأه لي بس عشان أربط حسابك بالخادم الجديد.
. والموضوع مستعجل لأنني أقفل التذكرة الساعة أربع
الموظف: طيب... بس ليش ما وصلني بريد عن الموضوع؟
المتصل: لأن البريد نفسه فيه الخلل، وهذا سبب اتصالي. وبعدين أبو خالد مدير الإدارة
. عندكم أعطاني أسماء القسم، وكلهم تعاونوا معي
(الرقم الطاهر يبدأ بـ 011)

#	العنصر	التصنيف (خ / م / س)
1	المتصل يعرف اسمك وإدارتك	
2	طلب قراءة رمز التحقق	
3	التخويف من تعطل البريد أمام المدير	
4	«مهلة» الساعة أربع	
5	تبرير غياب البريد الرسمي بالخلل نفسه	
6	«ذكر اسم مدير الإدارة وأن الزملاء» تعاونوا	
7	المتصل يتحدث باللهجة المحلية وبثقة	

#	العنصر	التصنيف (خ / م / س)
8	الرقم الظاهر يبدأ بمفتاح الرياض 011	

الإجراء الأنسب:

- (أ) أقرأ له الرمز، فهو يعرف مديري وزملائي.
- (ب) أرفض إعطاء الرمز، وأنهى المكالمة بلطف، وأتصل بالدعم الفني على رقمه الرسمي، وأبلغ الأمن عن المكالمة.
- (ج) أطلب منه رقم التذكرة، فإن أعطانيه قرأت له الرمز.
- (د) أرفض إعطاء الرمز وأنهى المكالمة.

الجزء الثالث: تحليل حالات حقيقية

ثلاث هجمات موثقة وردت في البرنامج، نجحت كلها بقرار بشري لا بثغرة تقنية. أجب عن الأسئلة الأربعة لكل حالة في سطرين إلى ثلاثة. كل حالة 8 درجات (4 أسئلة × درجتان).

الحالة الأولى: شركة يوبيكويتي (2015)

تلقي موظفون في الإدارة المالية رسائل بريد تتحل صفة مسؤولين تنفيذيين في الشركة، تطلب تحويلات عاجلة إلى حسابات خارجية لصفقات «سرية». نفذ الموظفون التحويلات، وبلغ مجموعها نحو 46.7 مليون دولار.

الحالة الثانية: أرامكو السعودية (2012)

فتح موظف رسالة احتيالية، فتمكن المهاجمون من الوصول إلى الشبكة ونشر برنامج تخريبي مسح بيانات نحو 30 ألف جهاز، وتعطلت أعمال إدارية لأسابيع.

الحالة الثالثة: شبكة كهرباء أوكرانيا (2015)

تلقي موظفون في شركات توزيع الكهرباء رسائل تصيد موجهة تحمل مستندات مكتوبة بمرفقات خبيثة. بعد أشهر من التسلل، تحكّم المهاجمون عن بعد في أنظمة التوزيع، فانقطعت الكهرباء عن نحو 225 ألف مشترك.

أسئلة التحليل (لكل حالة)

1. **الأسلوب والقناة:** ما أسلوب الهندسة الاجتماعية المستخدم (تصيد، ذريعة، طُعم، مقايضة)؟ وعبر أي قناة؟
2. **المحفز النفسي:** ما الدافع النفسي أو التحيز المعرفي الذي استغله المهاجم؟ استشهد بتفصيل من الحالة.
3. **نقطة الانكسار:** ما القرار البشري الواحد الذي فتح الباب للمهاجم؟

الضابط السلوكي: لو كنت في موقع ذلك الموظف داخل جهتك، ما الإجراء الذي كان سيوقف 4. الهجوم؟ وماذا تفعل لو اكتشفت الخطأ بعد وقوعه؟

سلم التقدير

الدرجة	الوصف
0	لا إجابة، أو إجابة خاطئة، أو عامة لا ترتبط بالحالة («يجب الانتباه»)
1	إجابة صحيحة جزئياً: تسمّي المفهوم دون دليل من الحالة، أو تقترح ضابطاً تقنياً فقط
2	إجابة دقيقة: تسمّي المفهوم وتربطه بتفصيل من الحالة، وتقترح إجراءً سلوكياً قابلاً للتطبيق في الجهة

يصحّح هذا الجزء مقيّمان مستقلان، ويُعتمد متوسط درجتهما. إذا تجاوز الفرق بينهما درجتين في الحالة الواحدة، يُحسم بمقيّم ثالث.

الجزء الرابع: السلوك المعلن والقنوات

ضع أمام كل عبارة رقماً يعبر عن مدى انطباقها عليك: 5 موافق بشدة 4 موافق 3 محايد 2 غير موافق 1 غير موافق بشدة. صِف ما تفعله فعلاً، لا ما ينبغي فعله.

#	العبارة	الدرجة (1-5)
	أ. السلوك اليومي	
1	أتحقق من عنوان المرسل الكامل قبل فتح أي رابط أو مرفق.	
2	أقفل شاشة جهازي كلما ابتعدت عنه، ولو لدقيقة.	
3	أستخدم كلمة المرور نفسها لأكثر من حساب لتسهيل تذكرها.	
4	أبلغ عن الرسائل المشبوهة عبر القناة المعتمدة حتى لو لم أنقر عليها.	
5	أؤجل تحديثات الأنظمة عندما أكون مشغولاً.	
6	أتحقق عبر قناة ثانية قبل تنفيذ أي طلب مالي أو طلب بيانات حساسة.	
7	أستخدم تطبيقات أو مواقع غير معتمدة لإنجاز العمل حين تكون الأدوات الرسمية بطيئة.	
8	أسمح لمن خلفي بالدخول إلى المناطق المقيدة إذا بدا موظفاً.	

#	العبارة	الدرجة (1-5)
	ب. القابلية والخطورة المدركة	
9	من غير المرجح أن يستهدفني المهاجمون، فعملي لا يهمهم.	
10	خطأ واحد مني قد يتسبب في تعطيل خدمة حيوية.	
11	جهات في قطاعي تعرضت لهجمات بدأت بخطأ بشري، وقد يتكرر ذلك عندنا.	
12	لدينا أنظمة حماية قوية، لذا لا داعي لقلقي الشخصي.	
	ج. الفوائد والعوائق المدركة	
13	الإجراءات الأمنية تعطل عملي أكثر مما تحمي.	
14	التحقق الثنائي يحمي حسابي فعلاً حتى لو سُرقَت كلمة المرور.	
15	وقت التحقق من الرسالة المشبوهة يستحق الجهد الذي يتطلبه.	
16	خطوات الإبلاغ عن الحوادث عندنا معقدة أو غير واضحة لي.	
	د. الكفاءة الذاتية	
17	أستطيع التمييز بين رسالة حقيقية ورسالة تصيد متقنة.	
18	أعرف بالضبط ماذا أفعل في الدقائق الأولى إذا شككت أن جهازي اختُرق.	
19	أستطيع رفض طلب مشبوه من شخص يبدو ذا منصب دون أن أشعر بالحرج.	
20	أشعر بالارتباك عند التعامل مع إعدادات الأمان في أجهزتي.	
	هـ. المعايير الاجتماعية والثقافة	
21	مديري المباشر يلتزم بالإجراءات الأمنية أماناً.	
22	زملائي يرون الإبلاغ عن الأخطاء الأمنية سلوكاً طبيعياً لا عيباً.	
23	لو أخطأت خطأً أمنياً سأتردد في الإبلاغ خوفاً من العقاب.	
24	يُقدَّر الموظف في إدارتي عندما يكتشف تهديداً ويبلغ عنه.	
	و. بندا صدق الاستجابة (لا يدخلان في الدرجة)	
25	لم أرتكب أي خطأ أمني مطلقاً طوال عملي.	
26	أقرأ كل سياسة أمنية تصلني كاملة فور وصولها.	

الجزء الخامس: التجارب الميدانية

ما يقوله الموظف في الاستبيان لا يكفي؛ هذا الجزء يرصد ما يفعله فعلاً دون أن يعلم بالتوقيت. تُنفَّذ التجارب على مدى ربع سنة، وتُعرض نتائجها مؤشراً مستقلاً بجانب درجة المقياس.

المستهدف الإرشادي	المؤشر	التصميم	السلوك المقاس	التجربة
نقر أقل من 10%، إبلاغ 40% فأكثر، أول بلاغ خلال 15 دقيقة	معدل النقر، معدل الإبلاغ، زمن أول بلاغ	ثلاث رسائل بصعوبة متدرجة: عامة، ثم موجهة باسم إدارة داخلية، ثم مخصصة خالية من الأخطاء	النقر، إدخال البيانات، الإبلاغ	محاكاة تصيد بالبريد
إفصاح 0%، إبلاغ 50% فأكثر	نسبة من أفصح، نسبة من أبلغ	اتصال من «الدعم الفني» على عينة عشوائية	الإفصاح عن رمز التحقق أو كلمة المرور	محاكاة تصيد صوتي
توصيل أقل من 5%، تسليم 50% فأكثر	نسبة التوصيل، نسبة التسليم للأمن	تسجل USB ذواكر التوصيل فقط دون أي أثر على الجهاز، تُترك في أماكن عامة داخل المبنى	توصيل وسائط مجهولة	اختبار الطُّعم
اعتراض 90% فأكثر	نسبة من اعترض أو وجهه للأمن	شخص من فريق الأمن المادي يحاول الدخول خلف الموظفين إلى منطقة مقيدة	السماح بالدخول خلف الموظف	اختبار التتبع
5% أقل من 5	نسبة الأجهزة غير المقفلة والمستندات الحساسة المتروكة	جولة بعد الدوام وأثناء أوقات الاجتماعات	ترك الأجهزة مفتوحة والمستندات مكشوفة	تدقيق المكتب والشاشة النظيفة

الدرجة الفردية (اختيارية)

في كل تجربة يتعرض لها الموظف: سلوك آمن مع إبلاغ = 2، سلوك آمن دون إبلاغ = 1، سلوك غير آمن = 0. تُجمع الدرجات وتُحوّل إلى نسبة مئوية من أقصى درجة ممكنة لعدد التجارب التي تعرّض لها.

ضوابط أخلاقية إلزامية

- يُعلن في سياسة الجهة أن المحاكاة جزء من برنامج التوعية، دون الإعلان عن توقيتها.
- يحصل التصميم على موافقة الإدارة القانونية والموارد البشرية والأمن السبراني قبل التنفيذ.
- من يقع في المحاكاة يرى فوراً صفحة تعليمية قصيرة، لا رسالة توبيخ، ولا تُنشر أسماء.