Almada
برمجيات وأمن

عرض فني مقدّم للجهات الحكومية والمؤسسات

برنامج التوعية الأمنية وتدريب الموظفين

رفع جاهزية العنصر البشري لمواجهة التصيد الاحتيالي والهندسة الاجتماعية وحماية البيانات الرسمية، بنتائج تُقاس قبل التدريب وبعده.

مقدّم إلى _____

رقم المرجع _____

التاريخ _____

المدى · طرابلس، ليبيا

almada.biz · info@almada.biz

01

المقدمة

تعتمد الجهات الحكومية والمؤسسات اليوم على البريد الإلكتروني والأنظمة الرقمية في مراسلاتها وخدماتها، وأصبح موظفوها الهدف الأول للمهاجمين. فأغلب الحوادث الأمنية لا تبدأ بثغرة تقنية، بل برسالة مقنعة أو مكالمة تنتحل صفة جهة رسمية أو مسؤول.

تقدّم المدى في هذا العرض برنامجاً متكاملاً للتوعية الأمنية وتدريب الموظفين، يجمع بين الورش التفاعلية ومحاكاة التصيد الآمنة والقياس الموضوعي للنتائج، ويُكيَّف مع طبيعة الجهة ومستويات موظفيها كافة.

البرنامج في سطور

4
مسارات تدريبية حسب الدور الوظيفي

5
مراحل تنفيذ من التقييم إلى المتابعة

قبل / بعد
قياس موضوعي للتحسّن بتقرير للإدارة

+4
لغات تدريب: العربية والإنجليزية والتركية والفرنسية وغيرها

عن المدى

المدى شركة ليبية مقرها طرابلس، تعمل في تطوير البرمجيات والأمن السيبراني. من أعمالنا نظام CACUS لكشف رسائل التصيد الاحتيالي، ونقدّم خدمات تقييم الأمن وفحص المواقع والتوعية الأمنية للجهات الحكومية والخاصة.

02

أهداف البرنامج

01 رفع قدرة الموظفين على كشف رسائل التصيد في البريد والرسائل النصية وتطبيقات المراسلة.

02 تمكين الموظفين من الصمود أمام أساليب الهندسة الاجتماعية، حتى تحت الضغط أو باسم السلطة.

03 ترسيخ الانضباط الأمني اليومي وفق معايير أمن المعلومات المعتمدة.

04 نشر ثقافة تصنيف البيانات وتحديد ما يمكن مشاركته ومع من وبأي قناة.

05 تمكين الإدارة العليا من تقييم المخاطر واتخاذ القرار السليم أثناء الحوادث.

06 بناء ثقافة إبلاغ مبكر عن الحوادث والرسائل المشبوهة دون حرج.

الفئات المستهدفة

الإدارة العليا والقيادات

الموظفون الإداريون والماليون

موظفو خدمة الجمهور والاستقبال

فرق تقنية المعلومات

الموظفون الجدد

الهيئات التدريسية والطلاب (للمؤسسات التعليمية)

المسارات التدريبية

المسار	الفئة	المدة المقترحة	المحاور الرئيسية
التوعية العامة	جميع الموظفين	ورشة 3 ساعات	كشف التصيد، كلمات المرور والتحقق بخطوتين، تصنيف البيانات ومشاركتها، الإبلاغ عن الحوادث.
القيادات	الإدارة العليا	جلسة إحاطة ساعتان	تقييم المخاطر، الاحتيال الموجّه للمسؤولين وانتحال صفتهم، القرار أثناء الحادث، المسؤولية القانونية والسمعة.
الفرق التقنية	تقنية المعلومات	يومان	السياسات الأمنية، الإدارة الآمنة للأنظمة والحسابات، كشف الحوادث والاستجابة لها، حماية البريد.
المستجدّون	الموظفون الجدد والطلاب	ساعتان	الأمان الرقمي الشخصي، وسائل التواصل الاجتماعي، حماية الحسابات والأجهزة.
محاكاة التصيد	الفئات المتفق عليها	حملة 4–6 أسابيع	رسائل تصيد تجريبية آمنة بموافقة مكتوبة، وقياس نسب الضغط والإبلاغ قبل التدريب وبعده.

المدد المذكورة مقترحة، وتُعدَّل حسب احتياج الجهة وعدد المتدربين.

المحاور التفصيلية

- التصيد في البريد والرسائل النصية وواتساب
- بروتوكول «توقّف · تحقّق · بلّغ» تحت الضغط
- كلمات المرور والتحقق بخطوتين
- تقييم المخاطر اليومية
- الهندسة الاجتماعية: السلطة والاستعجال والخوف
- تصنيف البيانات وقواعد المشاركة
- الأجهزة الشخصية ووحدات USB والعمل عن بُعد
- التصرف عند الحادث والإبلاغ

04

منهجية التنفيذ

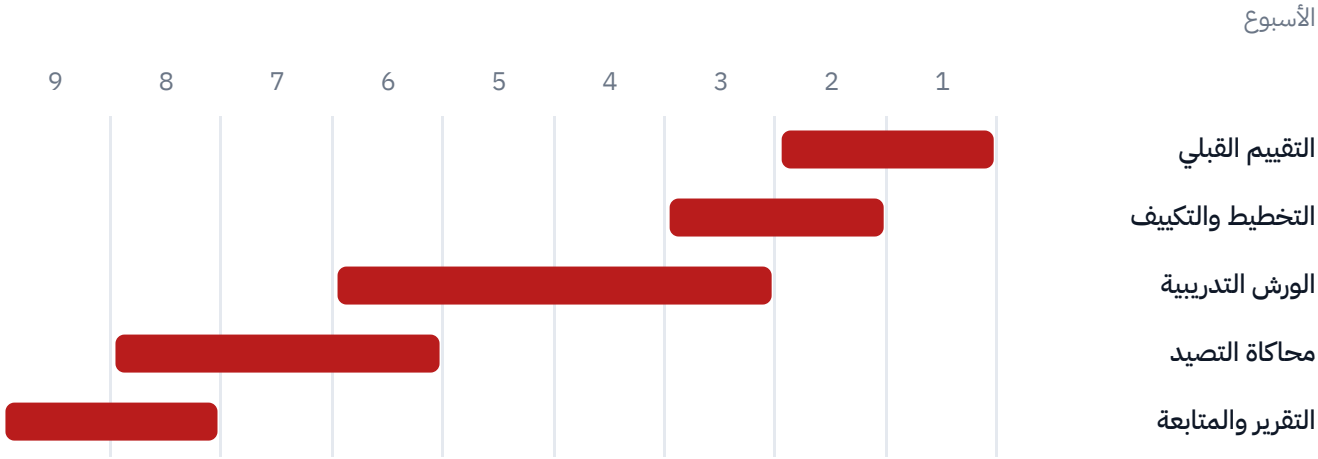
01 **التقييم القبلي**
استبيان قصير ومحاكاة تصيد أولية (اختيارية) تحدد مستوى الوعي الحالي لكل إدارة.

02 **التخطيط والتكييف**
تكييف المحتوى والأمثلة مع طبيعة الجهة وأنظمتها ولغة موظفيها، واعتماد الجدول.

03 **الورش التدريبية**
ورش تفاعلية بأمثلة واقعية من المنطقة، وتمثيل أدوار، وتمارين عملية.

04 **محاكاة التصيد**
حملة تجريبية آمنة تقيس ما تم تعلّمه في ظروف حقيقية.

05 **التقرير والمتابعة**
تقرير قبل/بعد للإدارة، وتوصيات، وخطة تذكير دورية.



جدول زمني نموذجي لجهة متوسطة الحجم؛ يُختصر أو يُمدَّد حسب عدد المتدربين.

05

المخرجات

- تقرير التقييم القبلي لكل إدارة
- مواد تدريبية مكيّفة للجهة بالعربية (ولغات أخرى عند الطلب)
- ورش تدريبية حسب المسارات المعتمدة
- حملة محاكاة تصيد آمنة وتقرير نتائجها
- تقرير ختامي قبل/بعد للإدارة العليا مع توصيات
- شهادات حضور للمتدربين
- دليل توعية مختصر وملصقات للتوزيع الداخلي

مؤشرات القياس

نسبة الضغط على روابط التصيد	تنخفض بين المحاكاة الأولى والثانية
نسبة الإبلاغ عن الرسائل المشبوهة	ترتفع بين المحاكاة الأولى والثانية
نتيجة التقييم المعرفي	تُقارن قبل التدريب وبعده لكل إدارة
نسبة الحضور والإكمال	لكل مسار تدريبي

السرية وحماية البيانات

- الالتزام باتفاقية عدم إفصاح (NDA) قبل بدء العمل.
- لا تُنفَّذ محاكاة التصيد إلا بموافقة مكتوبة من الجهة.
- لا تُجمع أي كلمات مرور أو بيانات حقيقية أثناء المحاكاة.
- تُسلَّم النتائج كملخصات دون أسماء ما لم تطلب الجهة غير ذلك.
- تُحذف بيانات المحاكاة بعد تسليم التقرير الختامي.

06

فريق التدريب

مؤهلات أكاديمية

أغلب أعضاء الفريق أكاديميون حاصلون على شهادات عليا في تخصص الأمن السيبراني.

خبرة بحثية وتطبيقية

خبرة في أبحاث كشف التصيد الاحتيالي وتطوير أنظمته، وفي تقييم أمن الأنظمة والمواقع.

تعدد اللغات

التدريب بالعربية والإنجليزية والتركية والفرنسية ولغات أخرى.

لكل المستويات

خبرة في تبسيط المفاهيم لغير التقنيين، من القيادات إلى الموظفين الجدد والطلاب.

طرق التقديم

حضورياً في مقر الجهة

عن بُعد، مباشرة عبر الإنترنت

مختلط (حضوري وعن بُعد)

برنامج سنوي بجلسات دورية

07

الأساس المالي

يُقدَّم العرض المالي منفصلاً بعد تحديد نطاق العمل، ويُحتسب على الأسس التالية:

البند	أساس الاحتساب
الورش التدريبية	حسب عدد المتدربين وعدد المسارات
محاكاة التصيد	حسب عدد المستهدفين وعدد الحملات
التقييم والتقارير	مشمولة في البرنامج المتكامل
البرنامج السنوي	قيمة سنوية تشمل الجلسات الدورية والمحاكاة والتقارير

تتوفر أسعار خاصة للجهات الحكومية والمؤسسات التعليمية.

ما نحتاجه من الجهة

- تسمية منسّق من الجهة للتواصل والمتابعة
- قاعة تدريب مجهّزة بجهاز عرض (للتدريب الحضوري)
- قائمة بالفئات وأعداد المتدربين
- الموافقة المكتوبة على محاكاة التصيد ونطاقها

الخطوات التالية

1. اجتماع تعريفي قصير لفهم احتياج الجهة
2. تحديد النطاق والمسارات وعدد المتدربين
3. إرسال العرض المالي والجدول الزمني
4. توقيع الاتفاق وبدء التقييم القبلي

08

للتواصل

العنوان
طريق 11 يونيو، الفرناج، طرابلس، ليبيا

الهاتف / واتساب
+218 91 020 0020

البريد الإلكتروني
info@almada.biz

الموقع
almada.biz/ar/security/awareness

الاعتماد

	عن الجهة	عن المدى
الاسم		
الصفة		
التوقيع		
التاريخ		

هذا العرض الفني عام ويُستكمل بعرض مالي وجدول زمني مخصّصين للجهة.