100 مقال

متخصص في أمن المعلومات

د. خالد بن سليمان الغثبر

استشاري و أستاذ أمن المعلومات المشارك

كلية علوم الحاسب الآلي و المعلومات بجامعة الملك سعود

ghathbar@ccis.ksu.edu.sa

1431

ضوابط عامة لكتابة المقال

ضوابط عامة لكتابة المقال

1. أن يكون المقال متخصص في مواضيع أمن المعلومات تشرح (مفاهيم،طرق،تعليمات،منتجات مُعينة).
2. أهمية إمتاع القارئ والاجتهاد في صياغة المقال بالشكل المناسب.

3. أن تكون لغة المقال باللغة العربية وتدقيق المقال لغوياً ونحوياً.
4. عَدم ترجمة المقال حرفياً أو النسخ من الإنترنت حرفياً إلا بالإشارة للمصدر وتحديد النص بعلامة التنصيص وكتابة المصادر في آخر المقال.
5. تعريف المصطلحات والاختصارات التقنية والتخصصية.
6. مراعاة ترابط النص (تسلسل الأفكار).
7. الدقة و الموثوقية للمعلومة المتضمنة في المقال، وعدم الاعتماد على المصادر الغير موثقة مثل المنتديات وغيرها.
8. أهمية التركيز على حداثة المعلومات.
9. الشمولية وجودة الموضوعية في الكتابة.
10. التنويع في المصادر المستفاد منها لكتابة المقال (كتب،مجلات،مواقع متخصصة....)
11. تحديد كلمات رئيسة افتتاحية.
12. أن يشمل المقال وسائل توضيحية (صور، رسومات،جداول)
13. أن يحتوي حجم المقال بين 1200 كلمة و 2000 كلمة مكتوبة باستخدام برنامج ميكروسوفت وورد،بمسافة مفردة بين السطور، مع محاذاة الأسطر من اليمين واليسار وترك هوامش مناسبة.
14. الهوامش: العلوي والسفلي = 2.54 سم والأيمن والأيسر = 3.18 سم.
15. الخط المستخدم: TIMES NEW ROMAN بحجم 12 لكامل المقال ، حجم خط العنوان: 20 متوسط في السطر وثقيل. (أما بالنسبة للعناوين الفرعية يجب أن لا يتجاوز الحد 20 والحد الأدنى 12)
16. الصور: تكون ذات جودة عالية وبصيغة jpg
17. يحفظ المقال بصيغة وورد.
18. الأخذ بالاعتبار بأن المقالات المتميزة سيتم نشرها عبر موقع التميز لأمن المعلومات تحت عنوان http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles.html
19. مراعاة حقوق الملكية الفكرية والتقييد بالضوابط العلمية في الاقتباس واستخدام المراجع.
20. التركيز على المفاهيم أكثر من المنتجات.

مقال نموذجي

- صفحة غلاف، تتضمن عنوان المقال.
- جدول المحتويات.
- نظرة عامة "ملخص" (٣٠٠ – ٢٠٠ كلمة).
- مقدمة، وتشمل:
  - الأهمية
  - الأهداف
  - اصل مشكلة المقال
  - مخرجات الورقة والمستفيدين منها
- محتوى المقال التفصيلي
- الخلاصة
- المراجع
- الملحقات
- معلومات الكاتب

عنواين المقال

1. نظرة عامة على تقييم التهديدات والمخاطر
2. Dll Hijacking
3. Evil twin attack
4. طرق اكتشاف والحماية من البرامج الخبيثة
5. كيف يفكر(الهكر والكراكرز) دراسة اجتماعية

6. مخاطر الـ كوكيز cookies
7. عالم Metasploit؟
8. ثغرت DoS في نظام Mac
9. مخاطر الـAd Aware
10. مشاكل وراء الـ Rootkit
11. التخطيط لأمن المنشئات والأجهزة الهامة
12. الرقابة من الأمن المادي والتخطيط للطوارئ
13. الأمن المادي واستمرارية العمل
14. المخاطر في النسخ الاحتياطي على الانترنت
15. سياسة الاحتفاظ بالبيانات الإلكترونية
16. اعتبارات أمن الحاسوب والأجهزة الأخرى في التخطيط للكوارث
17. الاحتياجات اللازمة لتصميم مركز بيانات آمن
18. أجهزة تتبع الأجهزة المسروقة عن بُعد
19. تهديدات الـWiFi
20. المشاكل الأمنية في أجهزة iPad
21. الخصوصية في أجهزة iPhone
22. سياسة الأمن المعلوماتي في استخدام الأجهزة المحمولة في بيئات العمل
23. معضلة الأمن النعلوماتي في أجهزة الـPDA
24. أمن قواعد البيانات
25. طرق حماية الملفات الخاصة و الحساسة
26. الخصوصية في الصفحات الاجتماعية
27. ثقافة الخصوصية لدي المجتمع العربي
28. التقنيات المستخدمة في خصوصية البيانات
29. مقارنة لثلاثة شركات ضمان الخصوصية عبر الانترنت مثال: TRUSTe و WebTrust
30. استخراج البيانات من شبكة الإنترنت لتأمين الأعمال
31. قضايا الأمن المعلوماتي في استخراج البيانات
32. التحليل المتقدم في أمن الحاسب
33. تقنيات التحليل المتقدم في استخراج البيانات من أجل الأمن والعدالة الجنائية
34. تطبيق أمان من عوامل التحقق معاً Two-Factor Authentication
35. أنظمة التشغيل وتطبيق تقنيات البصمة
36. مقدمة في إدارة الهوية Identity Management
37. كيفية تصنيف المعلومات
38. استخدام نظام التشغيل Linux في علميات المراجعة
39. تقنيات ذكية لمنع سرقة الهوية
40. Web Single Sign-On
41. قضايا مشتركة في تطبيق الـ PKI
42. أساليب المخترقين
43. الخداع داخل الانترنت
44. الصفحات الملغومة
45. المخاطر في URL Shortener
46. مقارنة في أمن المتصفح "Firefox VS Windows Internet Explorer "
47. تأثير الجرائم الالكترونية على النواحي الاقتصادية
48. هوية المجرم الالكتروني
49. معدلات الجريمة الإليكترونية
50. تقنيات الأدلة الجنائية الإلكترونية

عنواين المقال

51. معمل الأدلة الجنائية
52. دعم المصادر المفتوحة لعلم الأدلة الجنائية الكترونية
53. التحليل الجنائي للبرامج الخبيثة
54. التحليل الجنائي للهاتف الجوال
55. التقنيات والأدوات اللازمة لاستعادة وتحليل البيانات من الذاكرة المتطايرة
56. التحليل الجنائي لـ SQL Server
57. شرح مفصل لأفضل ثلاثة برامج من جدار الحماية (firewall) لعام 2010
58. نظام مكافحة الاقتحام SNORT
59. مقدمة في بروتوكولات الأمان
60. تقنيات مسح منافذ الشبكة والطرق الدفاعية
61. Network -Based Vulnerability Assessments
62. تصميم شبكة منزلية آمنة
63. تحديات إدارة استخدام أنظمة مكافحة الاقتحام IDS في المؤسسات ألكبرى
64. كيفية صيانة الشبكة الآمنة
65. المضادات والأدوات المستخدمة للحد من أنظمة مكافحة الاقتحام IDS
66. مصيدة الـ"Honeypot "
Psychological Biometrics؟
السمات الحيوية في التنقلات بين الدول
69. مستقبل الـ Behavioral Biometrics
70. السمات الحيوية للصوت
71. حماية الهوية واعتماد البطاقة الذكية في المنشات السعودية
72. قزحية العين لتحديد الهوية
73. حماية كلمة المرور : ماذا يمكننا فعله؟
74. نصائح هامة لتقييم الأمن المادي في بيئة العمل
75. إرشادات أمنية لمستخدمي الهواتف الذكية
76. الوعي الأمني المعلوماتي لدى المجتمع السعودي
77. أدوات ونصائح للمساعدة في تأمين جهاز الكمبيوتر الخاص بك في المنزل
78. دليل السلامة لاستخدام الانترنت للأطفال
79. تخصص أمن المعلومات الواقع والمستقبل
80. تحليل الأمن والتوصيات لنظام Mac
81. أهمية التوعية الأمنية
82. تطوير ثقافة الأمن التوعوي
83. لمحة عامة عن القضايا الأمنية التي تواجه مستخدمي الحاسب الآلي
84. أساليب وتقنيات ناجحة لتنفيذ برنامج التوعية الأمنية
85. المعيار العالمي لأمن المعلومات ISO 27001
86. إدارة نظام أمن المعلومات ISO 17799
87. المسائل القانونية في المملكة العربية السعودية
88. تحديات نظام مكافحة الجرائم الإلكترونية السعودي
89. ثغرات الـ Database Disclosure بتطبيقات الـ ASP
90. الحماية بواسطة نظام التشغيل
91. تحسين الأمن المعلوماتي من خلال البرمجة
92. أسلوب وآلية وطرق منع الـ"Buffer Overflow Attack "
93. طرق الهجوم والدفاع في "SQL Injection "
94. خوارزمية التشفير DES
95. خوارزم التشفير MD5

عنواين المقال

96. التشفير بالطرق الكلاسيكية
97. التعمية بالمفتاح العام - Public Key Crypto Systems
98. دور القطاع المصرفي السعودي في تأمين التعاملات الإلكترونية
99. تطبيقات آمنة في عمليات الدفع الإلكتروني
100.قضايا أمن المعلومات في التجارة الإلكترونية