نصائح وتوجيهات لمستخدمي الإنترنت



◄تكمن أهمية الإنترنت الكبرى في إنّه يقوم مقام ثلاثة أجهزة في آنٍ واحدٍ، فهو يجمع بينوسائل الإعلام بكافة صورها: المرئية، المسموعة والمقروءة، فيمكنك سماع المذياع ومشاهدة التلفاز وقراءة الصحف والمجلات، بل ويقوم مقام الهاتف فيمكنك مخاطبة شخص ما في آي مكان في العالم صوتاً وصورة من خلال نظام التحدث المعروف بـ(تشات)، ويمكنك متابعة محاضرة ما في أي دولة صوتاً وصورةً عبر النقل المباشر للشبكة، والدخول في مناقشات وحوارات لإبداء الرأي في أية قضية أو مشكلة دون حسب، أو رقيب. ومن هذا المنطلق نقدم لكم هذه النصائح والتوجيهات حتى يتمكن الجميع من استخدام الإنترنت بشكل آمن وفعال. الإنترنت سلاح ذو حدين: أوّلاً: إيجابيات الإنترنت: 1- استخدام الإنترنت في مجال الدراسة والتعلم حيث تتوفر الكثير من الموسوعات والمراجع العلمية التي تشكل لهم مصدراً للمعلومات لكتابة الأبحاث والواجبات المدرسية. 2- تنمية مهارات الاستطلاع والتعلم الذاتي، حيث صاغت الإنترنت شكل جديد للتعليم والتعلم الاستكشافي المفتوح والمشوق. 3- تنمية مهارة الأسلوب التفاعلي والمشاركة بالمعلومات والآراء والتجارب. 4- تعلم فن البيع والشراء عبر التجارة الإلكترونية، وفن الإنتاج والتسويق الإلكتروني. 5- استكشاف العالم ومتابعة كل ما يطرأ عليه من مستجدات في جميع المجالات الثقافية والفنية والرياضية. 6- تتعلم اللغات الأجنبية المختلفة. 7- تنمية الهوايات والمهارات، كل بحسب اهتماماته وهواياته. 8- متابعة مستجدات الابتكارات والمكتشفات في جميع أنحاء العالم.. 9-

ممارسة الألعاب الجماعية، وأقصد هنا الألعاب التعليمية وألعاب الذكاء كالشطرنج بحيث تنمي فيهم روح المنافسة. 10- اكتساب أصدقاء على مستوى العالم من خلال المحادثة والمراسلة. 11- تعلم مهارات التواصل والحوار مع الجنسيات المختلفة والإطلاع على ثقافات الشعوب وعاداتها وقضاياها. 12- تعزيز اللغة العربية قراءة وكتابة حين يستخدم المواقع العربية وكذلك تقوية لغته الانجليزية في حال اطلاعه واستخدامه للمواقع الانجليزية. 13- التسلية والترفيه. 14- إمكانية استفادة ذوي الاحتياجات الخاصة من الإنترنت، فللمكفوفين مثلاً أجهزة ملحقة بالكمبيوتر تحول النصوص إلى مواد سمعية أو إلى شاشات تعمل بنظام برايل. ثانياً: سلبيات الإنترنت: 1- المواقع اللاأخلاقية التي تكثر وتتكاثر في الإنترنت والتي يتم نشرها ودسها بأساليب عديدة في محاولة لاجتذاب الأطفال والمراهقين إلى سلوكيات منحرفة ومنافية للأخلاق. 2- غواية الأطفال والمراهقين حيث يتم التحرّش بهم وإغواءهم من خلال غرف الدردشة والبريد الإلكتروني. 3- نشر مفاهيم العنصرية والتعصب والدعوة للعنف. 4- الدعوة لأفكار غريبة مناهضة لدِيننا ولقيمنا ومفاهيمنا والتي تعرض بأساليب تبهر المراهقين. 5- الدعوة للانتحار والتشجيع له من خلال بعض المواقع وغرف الدردشة. 6- الانغماس في استخدام برامج الاختراق الهاكرز والتسلل لإزعاج الآخرين وإرسال الفيروسات التخريبية والمزعجة. 7- مشكلة إدمان الإنترنت. والأمراض النفسية التي تنجم عن سوء استخدام الإنترنت مثل الاكتئاب والقلق. 8- جرائم القتل التي ترتكب من خلال غرف المحادثة الغريبة من قبل جماعات تدعو لممارسة طقوس معينة لفنون السحر تؤدي بالنهاية إلى قتل النفس. 9- التعرض لعمليات احتيال ونصب وتهديد وابتزاز. 10- الحياة في الخيال وقصص الحب الوهمية والصداقة الخيالية مع شخصيات مجهولة وهمية أغلبها تتخفى بأقنعة وأسماء مستعارة، موما يترتب على مثل هذه القصص من عواقب خطيرة. 11- ممارسة الشراء الإلكتروني دون رقابة من خلال استخدام البطاقات الائتمانية الخاصة بأحد الوالدين. 12- استخدام الأسماء وتقمص شخصيات غير شخصياتهم في غرف الدردشة وما يتبعه ذلك من اعتياد ارتكاب الأخطاء والحماقات واستخدام الألفاظ النابية. 13- التعب الجسدي والإرهاق والأضرار الصحية والتي يسببها الاستخدام الطويل للكمبييوتر والإنترنت. من ضرر للعيون والعمود الفقري والمفاصل والأعصاب وزيادة الوزن أو نقصان الوزن وغيرها من المخاطر الصحية الجسدية. نصائح وتوجيهات: حماية البريد الإلكتروني: · يمثل البريد الإلكتروني أحد أقوى وسائل الاتصال والتواصل بين المستخدمين في عصرنا الحالي حيث من النادر وجود أشخاص لا يملكون بريد إلكتروني شخصي على الإنترنت. مما جعله هدف من الأهداف

التي يسعى ورائها المخترقون سواء لسرقة المعلومات أو تخزينها. لذلك توجب إلقاء الضوء على بعض المخاطر التي قد تواجه بريدك الإلكتروني وكيفية الحماية منها. كلمة المرور:

· احرص على أن تضع كلمة مرور ليست بالسهلة لبريدك الإلكتروني حيث يصعب على المخترق تحميلها والوصول إليها. · يفضل أن تشمل كلمة المرور على الأرقام والحروف والرموز.

· احذر اعطاء كلمة المرور الخاصة بك لأي شخص حتى لا يتم التلاعب ببريدك. · المواظبة على تغيير كلمة المرور بشكل دوري من فترة إلى أخرى للحفاظ على أمن معلومات. المرفقات: تأكّد دائماً من فحص الملفات المرفقة على البريد الإلكتروني قبل تحميلها على جهاز الحاسب الآلي الخاص بك لاحتمال حمل تلك الملفات فيروسات أو برامج تجسس للحصول على المعلومات الشخصية وأمثلة بعض الملفات الضارة التي قد تحتوي على برامج تجسس أو فيروسات تحمل الامتدادات (bat-vbs-dll-exe-scr-pif). الرسائل الإحتيالية: تعتبر هذه الأنواع من الرسائل من الطرق المفضلة لدى المخترقين حيث يمكنه من خلالها سرقة البريد الإلكتروني ومن ثمّ المعلومات الشخصية، مثال على ذلك، أن توصل رسالة توهم مستلمها بأنها مرسلة من مزود خدمة الإنترنت أو مزود خدمة البريد الإلكتروني أو من البنك المحلي الذي يتعامل معه العميل ويطلب من صاحب البريد الإلكتروني تعديل البيانات الشخصية أو غيرها من البيانات الخاصة لوجود مشكلة فنية ويضع رابط إلكتروني وهمي شبيه بالرابط الصحيح وعند إرسال البيانات ترسل إلى المحتال ويقوم المحتال بإساءة استخدام تلك البيانات لأغراض مختلفة. استخدام أكثر من بريد إلكتروني: · يفضل الاشتراك في أكثر من بريد شخصي بحيث يكون أحداهما مخصص للمراسلات الشخصية وأخرى للمرسلات غير المهمة. · استخدام البريد الإلكتروني على الحاسب الشخصي إلا في حالات الضرورة حتى لا يتم التلاعب به بعد تسجيل الخروج. · عدم اعطاء البريد الشخصي الذي يحتوي على المعلومات الشخصية إلا للأشخاص الموثوق بهم. استخدام النص الخالي من رموز لغة الترميز (html): عند استلام رسالة إلكترونية ويكون محتواها خطوط بأحجام كثيرة وألوان مختلفة وصور ينصح بفتحها بصيغة والبرامج الملفات تخريب والثاني الخصوصية انتهاك لّ الأو خطرين لتفادي (plain txt) الخاصة حيث إنّ هذه الخطوط والرموز تكون محملة ببرامج تجسس أو فيروسات. خطوات لحماية شبكتك اللاسلكية: إذا كنت تملك شبكة لاسلكية في المنزل أو مكان العمل فعليك الحذر من الدخلاء الذين قد يستخدمون شبكتك اللاسلكية للدخول إلى مواقع مشبوهة أو القيام بارتكاب أيّة جريمة إلكترونية أو الاطلاع على ما تقوم به من تصفح على الانترنت لذا إليك هذه الخطوات لحماية شبكتك اللاسلكية: تغيير كلمة المرور: يجب التأكيد في البداية من تغيير كلمة المرور الخاص بالشبكة اللاسلكية فكل نوع من أنواع الراوتر يأتي باعدادات افتراضية وكلمة مرور معده مسبقاً لذا لابدّ من تغييرها. استخدام عناوين الـ(MAC): ينصح بتحديد

الأجهزة المسموح لها بالاتصال بالشبكة اللاسلكية وذلك بتسجيل عنوان كات الشبكة (MAC) لكل جهاز في اعدادت الراوتر، لعمل ذلك قم بطباعة الأمر ALL-IPCONFIG في COMMANDPROMPT ثمّ قم بنسخ العنوان المكون من اثني عشر خانه بعلامة () الموجود. إيقاف بث الـ(SSID) وتغيير معرف شبكتك اللاسلكية: الـ(SSID) هو اسم الشبكة والراوتر يقوم ببث اسم الشبكة وبذلك يعرف الآخرون بوجودها فإذا تم إيقاف البث يمنع ذلك المتطفلين من رؤية الشبكة اللاسلكية ويفضل تغيير اسم الشبكة قبل إخفائها حتى لا يعرف الدخلاء اسم الشبكة والاتصال بها. إيقاف شبكتك اللاسلكية عند عدم الاتصال: ينصح بإطفاء الراوتر عند عدم الاستخدام فذلك يقلل من احتمالية استخدام الدخلاء للشبكة واختراقها. نصائح لحماية جهازك الشخصي: تعتبر برامج الفيروسات والاختراق والتجسس من أخطر البرامج التي قد تدمر الحاسب الشخصي حيث تعتمد آلية عملها على اتلاف الملفات الخاصة أو الحصول عليها لإساءة استغلالها. لذا ينصح بالتالي: استخدام برامج مضادة للفيروسات من النسخ الأصلية: قم بتنصيب برامج مكافحة الفيروسات على الحاسب الشخصي لحمايته من أي عملية اختراق والتأكد من تحديث برامج مضاد الفيروسات بشكل مستمر. فحص المرفقات: التأكد دائماً من فحص الملفات المرفقة على البريد الإلكتروني قبل تحميلها على الحاسب الآلي والتأكد من خلوها من الملفات التي تحمل فيروسات قد تضر ببيانات الحاسب الشخصي. فحص وحدات التخزين الخارجية (CD ,Flash ,DVD): قم بفحص الأقراص المدمجة ووحدات التخزين الخارجية والتأكد من خلوها من الفيروسات قبل استخدامها على حاسبك الآلي ويفضل فحص وحدات التخزين المختلفة بعد استخدامها على أجهزة كمبيوتر أخرى قبل استخدامها على جهازك الشخصي لأنّه قد يحتوي الجهاز الآخر على فيروس قد ينتقل للجهاز الآخر. تحميل البرامج التجارية: ينصح بالاحتياطية: برامج التجارية وخاصة المجانية منها إلى بعد التأكد من مصداقية الجهة المنتجة للبرنامج، فقد تكون هذه البرامج محملة بفيروسات أو برامج اختراق تدمر الجهاز. النسخ الاحتياطية: تأكد كم حفظ الملفات الشخصية الهامة على وحدات تخزين خارجية لإمكانية الرجوع إليها عند الحاجة ولحمايتها من أي عملية تخريب في حالة إصابة الحاسب الآلي بأيّة فيروسات تخريبية. الدعايات الإلكترونية: الحذر من فتح نوافذ الدعايات التي تجذب المستخدمين لأنها قد تحتوي على برامج الفيروسات أو برامج التجسس التي قد تخترق الحاسوب الشخصي أثناء عملية فتحها أو تحميلها أو استخدامها.►