Como "notas para llevarnos" relativas a la charla sobre Nociones de seguridad informática para padres de jóvenes y adolescentes, tenemos estas:

1. Sobre la **tecnoadicción**: Debemos tener en cuenta que los adultos tenemos las mismas obsesiones, sólo que nos preocupan más las de los niños. El mejor tratamiento es la **prevención**.

   Somos los **modelos** de nuestros hijos, y ellos harán lo que nos vean hacer: cuando ponemos el teléfono en la mesa al sentarnos a comer, cuando atendemos al teléfono al conducir (les estamos enseñando a priorizar el teléfono frente a la seguridad)…

   ¿Qué podemos hacer?

   - Limitar el uso: ellos saben qué es lo que les gusta, lo que no saben hacer es controlar el tiempo que dedican, y como padres somos quienes debemos ponerles los límites (y ponérnoslos a nosotros mismos)
   - Debemos educarlos en valores:
   - Enseñarles a gestionar el tiempo: equilibrio entre deporte, relaciones sociales, ocio, deberes, nuevas tecnologías…
   - Inculcarles los valores del trabajo y el esfuerzo: no hay recompensa sin esfuerzo. Pero, ojo, NO hay premio por hacer sus obligaciones: deberes del colegio, ayudar en casa.
   - Trabajar las habilidades sociales: convivencia y respeto por los demás.
   - Entrenarles el autocontrol: el "ya" no sirve, deben aprender a esperar.

2. Sobre la **anorexia, bulimia y pro-SI** (daño auto-infligido). Las princesas Ana y Mía son trastornos de conducta alimentaria, un conjunto de factores biológicos, psicológicos y sociales, del que el 90% de los adolescentes afectados son chicas. Estos factores son:
   - biológicos: la genética influye respecto al estado de ánimo y al temperamento.
   - socioculturales: la imagen personal percibida ante los demás.
   - psicológicos: como un modo de solucionar las dificultades de personalidad y afrontar los problemas de la vida.

   ¿Qué podemos hacer?
   - Trabajar en el colegio con los adolescentes, **fomentándoles el amor propio y fortaleciendo su autoconfianza**. La prevención, sobre el pro-SI no sirve: ¿hablamos de ello en clase? Efecto llamada: les puede tentar el probar…
   - **Herramientas de control de acceso a contenidos** en los ordenadores de casa (control parental). El reunirse en grupo con jóvenes afines provoca una reafirmación de la conducta.

3. Sobre el **sexting**. Consiste en el envío de contenidos de tipo sexual (principalmente fotografías o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles. Se trata de contenidos muy íntimos, generados mediante la grabación de sonidos o imágenes propias en actitudes sexuales, desnudos o semidesnudos, normalmente con destino a una pareja sexual o amorosa,

aunque también en no pocas ocasiones a otros amigos, como un simple juego. Esto expone al creador o creadora de dichos contenidos a graves riesgos.

¿Por qué lo hacen?

- **Confían** plenamente en la discreción —cuando no en el amor eterno profesado— por parte del destinatario del envío
- Sienten cierta **presión de grupo** más la plenitud **hormonal**
- Las influencias y modelos sociales distan del recato: ***scarlettjohansoning***
- **Desconocen las consecuencias**
- La natural falta de percepción del riesgo que acompaña a la adolescencia y el espíritu transgresor desencadenan ciertos desafíos

4. Sobre el **ciberbullying**. Es el acoso entre iguales por difusión de contenido lesivo o difamatorio.

   Los patrones de conducta que pueden mostrar los afectados son, con carácter general, de exclusión y de aislamiento en los espacios físicos. Síntomas de esto podrían ser:

   - Parece deprimido. Ha perdido interés en cosas que antes le entusiasmaban, descuida su arreglo personal, hay cambios de humor, de patrón de sueño...
   - Evita a sus amigos. Para no tener que dar explicaciones, se aleja incluso de su pareja sentimental.
   - Sus calificaciones bajan. La angustia que le atormenta no le permite concentrarse en el estudio, el rendimiento académico baja notablemente.
   - Pierde interés en actividades sociales y deportivas. No le interesa asistir a fiestas, eventos escolares, ni encuentros deportivos, todos estos en los que con seguridad se encontraría con mucha gente conocida.
   - Se comunica menos con sus padres. A pesar de ser un comportamiento “normal” durante la adolescencia, en caso de estar sufriendo ciberbullying se acentúa, especialmente en lo tocante a mantener alejados a los padres de su vida “digital”.
   - Muestra síntomas de angustia o ansiedad al usar su ordenador o el móvil. Su estado de ánimo es de enojo constante, pero no se resiste a mantenerse conectado, lo que incrementa su irritabilidad en forma considerable.

   Esta situación de desequilibrio supera la capacidad de reacción del menor, colocándole en una situación de indefensión y vulnerabilidad.

   El anonimato, la no percepción directa e inmediata del daño causado y la adopción de roles imaginarios en la Red convierten al ciberbullying en un grave problema.

5. Sobre el **grooming**. Es el acoso ejercido por un adulto contra un menor de edad con el fin de conseguir un control emocional sobre él o ella para reducir sus inhibiciones y preparar el terreno para un abuso sexual, virtual o real.

   Proceso que puede durar semanas o meses. Fases:

   - Elaboración de lazos emocionales: se hacen “amigos”.
   - Obtención de datos personales, intercambiando los propios. Obviamente, los datos del adulto son falsos aunque correspondan a los de un niño de edad aproximada.

- Empleo tácticas para obtención de contenido sexual: por ejemplo, empieza el adulto con imágenes obtenidas de forma fraudulenta, compradas en el mercado negro…
- Inicio del chantaje: comienzan a exigir más material, amenazando con divulgar el que ya tienen al círculo del menor; llegan incluso a exigir un encuentro físico.

6. Sobre la **ingeniería social**. Obtención de información confidencial manipulando a los usuarios legítimos; el arte de hacer que facilitemos información privada que en principio no estamos dispuestos a divulgar. Y una técnica "especial" dentro de la ingeniería social es el **phising**, que se diferencia en cómo se obtiene la información, en este caso de modo fraudulento, engañándonos: mediante adjuntos infectados, vínculos a páginas maliciosas o mediante falsificación de páginas de acceso a los servicios (facebook, twitter, bancos…) ¿Qué podemos hacer?
   - No dejarnos engañar cuando nos pidan datos personales, contraseñas y demás. Los sitios y servicios serios NO lo hacen. Sospechemos de entrada.
   - Los adjuntos a los correos electrónicos, aunque vengan de conocidos –que pueden estar infectados o haber sido víctimas de robo de cuenta- los descargamos en una carpeta, pasamos el antivirus y luego, si no hay aviso de virus, los abrimos. Es tedioso, pero es lo seguro.
   - Antes de hacer clic en un hipervínculo dejamos el cursor del ratón sobre él, y veremos la dirección real; si no coinciden, no hacemos clic. Si no nos saliera la dirección, haríamos clic con el botón derecho del ratón sobre el hipervínculo, elegiríamos la opción de "copiar hipervínculo" y, abriendo el Notepad, por ejemplo, copiaríamos con botón derecho -> pegar y así veríamos la dirección real a que nos manda el hipervínculo.
   - Para acceder a páginas en que se nos pida usuario y contraseña NO usaremos nunca hipervínculos, y menos que nos manden en mensajes de error, aviso, peligro… Escribiremos nosotros la dirección en la barra correspondiente del navegador para evitar ir a páginas maliciosas donde recolectan nuestros datos para robarnos las cuentas de correo, redes sociales, etc.

MEDIDAS PREVENTIVAS DE CARÁCTER GENERAL

Tenemos que explicarles que tras el monitor hay un mundo virtual pero que no desaparece al apagar el ordenador sino que sigue "vivo" al igual que el real, con todo lo bueno y lo malo; pero que las consecuencias de lo que se hace en Internet se pagan aquí, que no desaparecen al apagar el ordenador. En Internet no existen el anonimato ni la impunidad: una cosa es no saber quién está al otro lado y otra, muy distinta, es que no se pueda saber; y que lo que se hace se paga.

Interesarnos por lo que hacen en Internet, ellos y sus amigos; pedirles que nos enseñen los sitios que visitan, no para "cotillear" sino para que perciban nuestro interés y nos sientan más cercanos. No nos importe perder media hora viendo cómo juegan en el Club Penguin, por ejemplo. Después podremos volver a esos lugares y comprobarlos más en profundidad, creándonos incluso perfiles nosotros mismos.

Y que como poco deben ser desconfiados: de los desconocidos sobre todo, de los vínculos y las súper-ofertas con que nos acosan, de los adjuntos "raros" que recibimos en el correo electrónico aún cuando provenga de conocidos…

Las imágenes pueden ser malempleadas y sacadas de contexto; con la información "delicada" estamos desnudándonos ante el mundo y haciéndonos más vulnerables.

Y ya que no vamos a dar esas imágenes ni esa información, velaremos porque no nos la puedan robar manteniendo actualizado todo el software del ordenador, que además ha de ser legal.

Sin llegar a ser neuróticos, intentar ir un paso por delante y pensar en cómo pueden utilizar los demás la información que publiquemos

Y esta charla con ellos repetirla una vez al año, para estar "al día" de su actividad en Internet.

MEDIDAS DE AFRONTAMIENTO

Tan pronto se reciban amenazas o chantaje:

- No ceder, no aumentar los datos/fotos que ya puedan tener nuestros.
- Pedir ayuda: hermanos mayores, profesores, padres…
- Evaluar la veracidad de la amenaza
- Revisar la seguridad del PC, teléfono; cambiar TODAS las claves acceso y contraseñas

Este es un paso difícil, pues el menor siente que es más fácil ceder al chantaje, con la vana esperanza de que se termine, a enfrentarse cara a cara con sus padres que, con probabilidad, no van a ser capaces de empatizar con su situación y le culparán de lo ocurrido cuando no es sino la víctima.

Puede ser que sientan a sus hermanos mayores más cercanos a ellos en esta situación, y un poco menos a los profesores; pero a los que sienten más lejanos es a los padres, a esos "inmigrantes digitales".

Una vez estemos al día de lo que le ocurre al menor, y con toda la serenidad del mundo, procederemos a averiguar si realmente el acosador dispone de los medios y la capacidad de ejecutar la amenaza.

Y realizaremos una revisión a fondo de la seguridad de todos los dispositivos: PC, teléfono, tablet… Como medida ineludible e inmediata cambiaremos todas las contraseñas de las cuentas, perfiles y servicios que tengamos, y revisaremos las configuraciones de privacidad de las aplicaciones, etc.

MEDIDAS DE INTERVENCIÓN

Difícilmente la situación acabe porque si, lo que nos obligará a tomar medidas legales.

Si se trata de un caso de ciberbullying se puede intentar dialogar con los acosadores y sus padres y pedirles que se deponga la actuación. De lo contrario estaremos al punto siguiente.

Buscaremos y recopilaremos cuantas pruebas podamos de la actividad delictiva: chats, mensajes intercambiados, pantallazos de páginas de las aplicaciones…

Y la última instancia sería formular la denuncia, aportando las pruebas recogidas en el punto anterior.

OTRAS MEDIDAS PREVENTIVAS

Con los dispositivos:

El ordenador

- En un lugar común de la casa. No aconsejado en los dormitorios
- Establecer momentos y periodos de empleo:
  - Ni después de cenar ni antes de acostarse
- Crear un perfil por usuario. Ni Administrador ni invitado, cada uno con su contraseña.
- Evaluar necesidad de aplicaciones de control parental:
  - Propio del sistema operativo: muy complejo de implantar
  - Propio del proveedor de Internet: fácil pero no configurable
  - Aplicaciones de terceros (WinLive Protección Infantil, Norton Family, K9 Web Protection, Qustodio…). La mejor opción si hay que llegar al control parental.
- El sistema operativo: legal y actualizado
- Un solo antivirus, también legal y actualizado. Las versiones gratuitas son suficientes.
- Resto de programas: legales y actualizados. Hay software libre para todo.
- Configurar los DNS para navegación segura/filtrada

Los navegadores:

- Navegar en modo incógnito
- Conectarse a través de protocolo seguro: https://www...
- Extensiones: bloqueo anuncios, alargador url…
- Anti-malware: adwcleaner, Malwarebytes, Spybot…
- Limpiador-optimizador de equipo: Ccleaner, Advanced System Care…

El router

- Cambiar usuario y contraseña de acceso al router
- WiFi:
  - Encriptación WPA/WPA2. Prohibida la WEP
  - Cambiar el nombre de la red WiFi.
  - Contraseña segura de acceso a la red WiFi
  - Dejar de difundir el nombre de la red: ocultarla
  - Desactivar WPS
- Configurar los DNS.

ALGUNOS SITIOS DÓNDE AMPLIAR INFORMACIÓN

http://www.pantallasamigas.net

http://www.privacidad-online.net

http://www.sexting.es

http://www.e-legales.net

http://www.cuidatuimagenonline.com

http://www.ciberbullying.com

http://www.kidsandteensonline.com

http://www.segu-kids.org

http://elblogdeangelucho.com

https://www.gdt.guardiacivil.es Aquí, además, podemos denunciar.

Contacto:

Twitter: @petruxIT

https://plus.google.com/+PedroGonzálezIT

Slideshare: www.slideshare.net/petruxIT