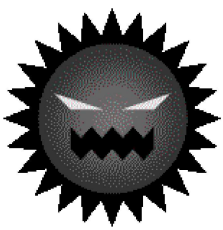


你们那儿并不是“公司里”！！



远程(在家)办公时



真的安全不安全??



譬如说…

常常发生这样的事…



通过网站或APP而感染电脑病毒
来被监听窃取信息。

~ 经常请更新最新的端末、机器、对策病毒软件。

在咖啡店等有的免费WiFi热点

会没那么安全，

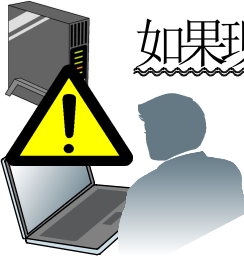
因此有可能性被监听窃取通信内容。



~ 通过WiFi热点(公共场所的WiFi)通信肯定有被监听窃取非常大的风险。除非把通信路径弄成加密化(VPN)，否则利用时，首先关闭“文件共享功能”，请尽量避免操作敏感功能(比如网银、购物或收发涉密邮件文件等)。

你们家的WiFi路由器的管理用账号和密码，

如果现在也没更新初始设定的话，有可能性会被侵入到电脑里。



~ 本来不记得更不更新…那样的话，请在路由器的管理画面上确认。现在也没更新「admin」或「password」等这样的初始设定的话，非常危险。请马上更新账号和密码让他人很难推测。

~ 其他 ~

- 请不要转用各个密码。
- 请在公共场所注意被偷看及被偷走信息。
- 请预先确认有关远程办公的问题发生时跟哪儿商量。

北海道警察
网络安全防御对策本部

网络安全防御广场

检索

温馨提示

免费Wi-Fi的危险性

在未被加密的通信 及 在不安全的通信
有可能性被监听窃取内容！

可以免费使用的，就是叫「免费Wi-Fi热点」，设置在很多场所，譬如说在咖啡店及公共场所等等。

免费Wi-Fi非常方便，但是没确认通信方法而使用的话，有可能性被监听或个人信息被窃取。

● 我们使用加密方式中安全性最好的吧！

加密方式的安全性

无

WEP

WPA

WPA2

WPA3

不好

好

确认加密方式的办法

安 卓

安卓，一般来说在选择SSID(服务集标识)而表示「安全性」的项目上可以确认。(表示「无」的是未加密的通信，所以一定要注意。)

iPhone

iPhone，接连免费Wi-Fi时，未加密的通信表示「没有被安全地保护的通信」、安全性不好的通信(WEP)表示「安全性不好的」。



未加密的通信

加密的通信
(注意一下安全性的强度)

如果使用未加密的通信或者安全性很坏的通信的话，有可能性被坏人监听窃取你的信息。

很容易监听窃取

通信内容

阅览情况、投稿情况、个人信息(账号·密码、名字、地址、电话号码、信用卡的信息)等等



北海道警察

网络安全防御对策本部

网络安全防御广场

检索

请亲自保护宝贵的信息吧！