

中华人民共和国最高人民法院
中华人民共和国最高人民检察院
公 告

最高人民法院、最高人民检察院《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》已于 2011 年 6 月 20 日由最高人民法院审判委员会第 1524 次会议、2011 年 7 月 11 日由最高人民检察院第十一届检察委员会第 63 次会议通过，现予公布，自 2011 年 9 月 1 日起施行。

2011 年 8 月 1 日

最高人民法院 最高人民检察院
关于办理危害计算机信息系统安全刑事案件
应用法律若干问题的解释

法释〔2011〕19号

(2011年6月20日最高人民法院审判委员会第1524次会议、2011年7月11日最高人民检察院第十一届检察委员会第63次会议通过 2011年8月1日最高人民法院、最高人民检察院公告公布 自2011年9月1日起施行)

为依法惩治危害计算机信息系统安全的犯罪活动，根据《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》的规定，现就办理这类刑事案件应用法律的若干问题解释如下：

第一条 非法获取计算机信息系统数据或者非法控制计算

机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

- （一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；
- （二）获取第（一）项以外的身份认证信息五百组以上的；
- （三）非法控制计算机信息系统二十台以上的；
- （四）违法所得五千元以上或者造成经济损失一万元以上的；
- （五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

- （一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；
- （二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

第二条 具有下列情形之一的程序、工具，应当认定为刑法第二百八十五条第三款规定的“专门用于侵入、非法控制计算机信息系统的程序、工具”：

- （一）具有避开或者突破计算机信息系统安全保护措施，未

经授权或者超越授权获取计算机信息系统数据的功能的；

（二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；

（三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具。

第三条 提供侵入、非法控制计算机信息系统的程序、工具，具有下列情形之一的，应当认定为刑法第二百八十五条第三款规定的“情节严重”：

（一）提供能够用于非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的专门性程序、工具五人次以上的；

（二）提供第（一）项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的；

（三）明知他人实施非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的违法犯罪行为而为其提供程序、工具五人次以上的；

（四）明知他人实施第（三）项以外的侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具二十人次以上的；

（五）违法所得五千元以上或者造成经济损失一万元以上的；

(六) 其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为提供侵入、非法控制计算机信息系统的程序、工具“情节特别严重”：

(一) 数量或者数额达到前款第(一)项至第(五)项规定标准五倍以上的；

(二) 其他情节特别严重的情形。

第四条 破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

(一) 造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；

(二) 对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；

(三) 违法所得五千元以上或者造成经济损失一万元以上的；

(四) 造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

(五) 造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏

计算机信息系统“后果特别严重”：

（一）数量或者数额达到前款第（一）项至第（三）项规定标准五倍以上的；

（二）造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（三）破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（四）造成其他特别严重后果的。

第五条 具有下列情形之一的程序，应当认定为刑法第二百八十六条第三款规定的“计算机病毒等破坏性程序”：

（一）能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；

（二）能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；

（三）其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

第六条 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，具有下列情形之一的，应当认定为刑法第二百八十六条第三款规定的“后果严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播的；

（二）造成二十台以上计算机系统被植入第五条第（二）、（三）项规定的程序的；

（三）提供计算机病毒等破坏性程序十人次以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（二）数量或者数额达到前款第（二）项至第（四）项规定标准五倍以上的；

（三）造成其他特别严重后果的。

第七条 明知是非法获取计算机信息系统数据犯罪所获取

的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒，违法所得五千元以上的，应当依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得罪定罪处罚。

实施前款规定行为，违法所得五万元以上的，应当认定为刑法第三百一十二条第一款规定的“情节严重”。

单位实施第一款规定行为的，定罪量刑标准依照第一款、第二款的规定执行。

第八条 以单位名义或者单位形式实施危害计算机信息系统安全犯罪，达到本解释规定的定罪量刑标准的，应当依照刑法第二百八十五条、第二百八十六条的规定追究直接负责的主管人员和其他直接责任人员的刑事责任。

第九条 明知他人实施刑法第二百八十五条、第二百八十六条规定的行为，具有下列情形之一的，应当认定为共同犯罪，依照刑法第二百八十五条、第二百八十六条的规定处罚：

（一）为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序、工具，违法所得五千元以上或者提供十人次以上的；

（二）为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算、交易服务、广告服务、技术培训、技

术支持等帮助，违法所得五千元以上的；

（三）通过委托推广软件、投放广告等方式向其提供资金五千元以上的。

实施前款规定行为，数量或者数额达到前款规定标准五倍以上的，应当认定为刑法第二百八十五条、第二百八十六条规定的“情节特别严重”或者“后果特别严重”。

第十条 对于是否属于刑法第二百八十五条、第二百八十六条规定的“国家事务、国防建设、尖端科学技术领域的计算机信息系统”、“专门用于侵入、非法控制计算机信息系统的程序、工具”、“计算机病毒等破坏性程序”难以确定的，应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验。司法机关根据检验结论，并结合案件具体情况认定。

第十一条 本解释所称“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

本解释所称“身份认证信息”，是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。

本解释所称“经济损失”，包括危害计算机信息系统犯罪行为给用户直接造成的经济损失，以及用户为恢复数据、功能而支

出的必要费用。