

ระวังอันตราย 5 ประการในเครื่องใช้คอมพิวเตอร์

นำเสนอเมื่อ : 29 ส.ค. 2552

ผู้ชายคนหนึ่งซึ่งอยู่ในนิวยอร์กอาจเข้าไปดูข้อมูลส่วนบุคคลของคุณ ซึ่งถ้าเป็นเช่นนั้น เขาอาจขโมยข้อมูลบัญชีธนาคารออนไลน์ของคุณ ปัจจุบัน Jiju Jiang ได้ชี้ให้เห็นสิ่งที่เขากระทำได้ หลังจากที่มีการตัดสินความผิด แต่ในช่วงหลายปีที่ผ่านมา เขาได้ใช้ซอฟต์แวร์ตรวจสอบแป้นพิมพ์เพื่อขโมยชื่อผู้ใช้และรหัสผ่านจากเครื่องคอมพิวเตอร์สาธารณะ ซึ่งเขาใช้ในการขโมยเงิน หรือขายข้อมูลนั้นบนเว็บ เขาถูกจับในขณะที่เขากำลังจัดการกับเครื่องคอมพิวเตอร์ที่บ้านของเหยื่อ

เธอจ่อมองวิธีการที่คนร้ายค้นหาเครื่องคอมพิวเตอร์ของเธออย่างไม่เชื่อสายตาตนเอง เขาใช้ GoToMyPC ซึ่งเป็นโปรแกรมสำหรับนักเดินทางที่สามารถจัดการเครื่องคอมพิวเตอร์ของคุณจากระยะไกลได้ เหยื่อรายนี้ได้ใช้ GoToMyPC กู้หนุหนานี้จากเครื่องสาธารณะ และ Jiang ได้ขโมยชื่อผู้ใช้และรหัสผ่านของเธอไป

เรื่องดังกล่าวได้สร้างความสนใจให้กับสิ่งที่ผู้คนเคยมองข้าม ซอฟต์แวร์ประเภทสปายแวร์สามารถติดตั้งลงในเครื่องคอมพิวเตอร์สาธารณะได้ง่าย เช่น อินเทอร์เน็ตคาเฟ่ สนามบิน ห้องสมุด และสถานที่สาธารณะอื่นๆ

อาชญากรสามารถขโมยชื่อผู้ใช้และรหัสผ่านของคุณไปได้โดยการใช้ซอฟต์แวร์ประเภทสปายแวร์ จากนั้นคุณอาจสูญเสียเงินหรือถูกขโมยข้อมูลเฉพาะตัว เรื่องต่างๆ เหล่านี้จะช่วยยืดเวลาให้คุณระมัดระวังในการใช้เครื่องคอมพิวเตอร์สาธารณะซอฟต์แวร์จะไม่เป็นที่สังเกตการณ์มากนัก

ใช้ซอฟต์แวร์เนื่องจากซอฟต์แวร์เป็นสิ่งที่คุณต้องระวังไปมากไม่สังเกตเห็น หรืออาจนำฮาร์ดแวร์มาวางไว้ระหว่างแป้นพิมพ์และเครื่องคอมพิวเตอร์ แต่การใช้ฮาร์ดแวร์จะเป็นที่สังเกตเห็นได้ง่ายในที่สาธารณะ

โปรแกรมเหล่านี้สามารถบันทึกการใส่แป้นพิมพ์โดยที่เหยื่อไม่ทันรู้ตัว จากนั้นจึงส่งข้อมูลที่บันทึกไว้ทางอีเมลตามเวลาที่กำหนด หรือใช้วิธีการดาวน์โหลดข้อมูลดังกล่าว โปรแกรมอื่นๆ อาจบันทึกภาพหน้าจอของเว็บไซต์ที่คุณเยี่ยมชม ข้อมูลที่บันทึกไว้เหล่านี้ก็จะถูกส่งทางอีเมลเช่นเดียวกัน

ดังที่กล่าวไว้ข้างต้น คุณจะสังเกตเห็นโปรแกรมประเภทสปายแวร์ เว้นแต่ว่าคุณจะทราบวิธีการค้นหา คุณจึงจะพบโปรแกรมเหล่านี้

คุณจึงควรตรวจสอบเครื่องคอมพิวเตอร์ของคุณว่ามีซอฟต์แวร์สปายแวร์อยู่หรือไม่ก่อนใช้งาน ซึ่งจะกล่าวในรายละเอียดต่อไป แต่อยากให้คุณตระหนักไว้ว่า นอกจากโปรแกรมสปายแวร์ คุณอาจพบกับภัยคุกคามอื่นๆ ซึ่งเลวร้ายยิ่งกว่าการใช้ห้องนำสาธารณะ! ขอควรพิจารณา 5 ประการเมื่อคุณใช้งานเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานเป็นประจำมีดังต่อไปนี้ การตรวจสอบโปรแกรมสปายแวร์

คุณสามารถดาวน์โหลด X-Cleaner Spyware Remover ได้จาก spywareinfo.com แล้วคัดลอกเก็บไว้ในฟลอปปีดิสก์ หากเครื่องคอมพิวเตอร์สาธารณะที่คุณใช้มีฟลอปปีดิสก์ ให้ใส่แผ่นดิสก์และเรียกใช้ X-Cleaner จากฟลอปปีดิสก์เพื่อตรวจสอบฮาร์ดดิสก์ โดยคุณไม่จำเป็นต้องติดตั้ง X-Cleaner การลบข้อมูลของคุณ เมื่อคุณใช้งานอินเทอร์เน็ตเบราว์เซอร์ ระบบจะบันทึกเว็บไซต์ที่คุณเยี่ยมชมเอาไว้

หลังจากที่คุณเรียกดูข้อมูลต่างๆ โดยใช้ Microsoft Internet Explorer เสร็จแล้ว ให้คลิก Tools > Internet Options ในแท็บ General ให้คลิก Delete Files และ Delete Cookies จากนั้นให้คลิก Clear History หากคุณใช้ Netscape Navigator การดำเนินการอาจซับซ้อนกว่าเล็กน้อย โปรดทำตามขั้นตอนต่อไปนี้

?คุณจะต้องตรวจสอบการตั้งค่าก่อนใช้งานออนไลน์โดยคลิก ที่ Edit และ Preferences แล้วคลิกที่ลูกศรที่อยู่หน้า Navigator และเลือก History จากนั้นให้มองหา Browsing History ทางด้านขวา แล้วเปลี่ยน "Remember visited pages" เป็น 0 ?คลิกลูกศรที่อยู่หน้า Privacy and Security แล้วเลือก Disable Cookies และ Disable Cookies in Mail and Newsgroups ?เมื่อคุณเรียกดูข้อมูลเสร็จแล้ว ให้คลิก Edit และ Preferences แล้วคลิกที่ลูกศรที่อยู่หน้า Navigator คลิก Clear History และ Clear Location Bar แล้วไปที่ Privacy and Security ทางด้านซ้ายและคลิกลูกศร เลือก Cookies คลิก Manage Stored Cookies ในแท็บ Stored Cookies ให้คลิก Remove All Cookies ?จากนั้นให้ไปที่ Advanced ที่อยู่ในบานหน้าต่างทางด้านซ้าย คลิกที่ลูกศร แล้วคลิก Cache คลิก Clear Memory Cache และ Clear Disk Cache การป้องกันรหัสผ่านของคุณ

เบราว์เซอร์สามารถตรวจสอบรหัสผ่านได้เช่นกัน ก่อนที่คุณจะใช้งานเว็บ หากคุณใช้ Internet Explorer ให้คลิก Tools > Internet Options ในแท็บ Content ให้คลิก AutoComplete แล้วยกเลิกการเลือกทั้ง 4 ช่อง เมื่อคุณเรียกดูข้อมูลเสร็จแล้ว ให้คลิก Tools > Internet Options แล้วไปที่แท็บ Content และคลิก AutoComplete คลิก Clear Forms และ Clear Passwords หากคุณใช้ Netscape ให้คลิก Edit และ Preferences คลิกลูกศรที่อยู่หน้า Privacy and Security แล้วคลิก Passwords ยกเลิกการเลือกในช่อง Remember Passwords เมื่อคุณเรียกดูข้อมูลเสร็จแล้ว ให้คลิก Passwords ใน Privacy and Security อีกครั้ง คลิก Manage Stored Passwords เลือกแท็บ Passwords Saved แล้วคลิก Remove All Netscape มีคุณสมบัติที่คล้ายกับ AutoComplete ซึ่งจะบันทึกข้อมูลที่ป้อนลงในฟอร์ม ในการปิดการใช้งาน คุณสมบัติดังกล่าว ให้คลิก Forms ใน Privacy and Security แล้วยกเลิกการเลือก "Save form data from Web pages when completing forms" เมื่อคุณเรียกดูข้อมูลเสร็จแล้ว ให้กลับไปยังหน้า Forms คลิก Manage Stored Form Data แล้วคลิก Remove All Saved Data

การลบข้อมูลในเบราว์เซอร์จะทำให้คุณแน่ใจได้ว่าผู้อื่นจะไม่สามารถตรวจสอบการเรียกดูข้อมูล หรือขโมยรหัสผ่านจากข้อมูลที่บันทึกไว้ได้

แต่โปรแกรมตรวจสอบการใช้แป้นพิมพ์ยังสามารถบันทึกที่กรหัสผ่านของคุณได้

โปรแกรมตรวจสอบการใช้แป้นพิมพ์บางโปรแกรมไม่สามารถบันทึกที่กรหัสผ่านของคุณไว้ได้

หากคุณป้อนรหัสผ่านโดยใช้การตัดลอกและวางตัวอักษรหรือตัวเลข ตัวอย่างเช่น

เพจที่คุณเปิดในเบราว์เซอร์มีตัวอักษรต่างๆ และสมมติว่ารหัสผ่านของคุณคือ "jim" (คุณคงไม่ใช่รหัสผ่านง่ายเช่นนี้!)

คุณสามารถค้นหาตัวอักษร "j" หนึ่งตัว "i" หนึ่งตัว "m" อีกหนึ่งตัวในเพจนั้น แล้วคัดลอกและวางลงในช่องรหัสผ่าน

การเข้ารหัสผ่านชั่วคราวอาจเป็นการป้องกันรหัสผ่านที่ดีที่สุด คุณอาจใช้รหัสผ่านสำหรับการทำงาน

และยกเลิกเมื่อสิ้นสุดการทำงาน อย่าเชื่อมั่นการเข้ารหัสข้อมูลมากเกินไป

โปรแกรมการเข้ารหัสมีอยู่มากมายในท้องตลาด บางโปรแกรมอาจใช้สำหรับการเข้ารหัสอีเมล อย่างไรก็ตาม

โปรแกรมเหล่านั้นจะเข้ารหัสข้อมูลเมื่อมีการคลิกที่ปุ่ม ส่ง

ซึ่งเป็นการป้องกันที่สายเกินไปหากมีการติดตั้งโปรแกรมตรวจสอบการใช้แป้นพิมพ์ในเครื่องคอมพิวเตอร์

โปรแกรมดังกล่าวจะบันทึกที่กรหัสผ่านและขอความที่คุณเขียนได้อย่างถูกต้อง การใช้วิจารณญาณที่ดี

การใช้เครื่องคอมพิวเตอร์สาธารณะอาจมีความปลอดภัย แต่คุณไม่สามารถมั่นใจได้เต็มที่

คุณสามารถติดตั้งระบบรักษาความปลอดภัยให้กับเครื่องคอมพิวเตอร์ที่บ้านหรือที่ทำงานได้

แต่คุณไม่สามารถมั่นใจได้ว่ามีอะไรแอบแฝงอยู่ในเครื่องสาธารณะนั้นหรือไม่

คุณควรใช้งานเครื่องเหล่านี้ด้วยความระมัดระวัง

อย่าทำธุรกรรมเกี่ยวกับการเงินหรือการซื้อขายหุ้นในเครื่องเหล่านี้หากคุณสามารถหลีกเลี่ยงได้

หลีกเลี่ยงการทำรายการที่ใช้ข้อมูลบัตรเครดิต และใช้รหัสผ่านชั่วคราวหากคุณต้องตรวจสอบอีเมล

รวมทั้งสอบถามผู้ดูแลระบบของคุณถึงวิธีการในการ "ยกเลิกการเรียกดูเพจ"

หากคุณใช้เครื่องคอมพิวเตอร์เพื่อเรียกดูข้อมูลเท่านั้น ซึ่งไม่น่าจะมีปัญหาใดๆ

คุณควรหลีกเลี่ยงการใช้ข้อมูลธุรกิจที่สำคัญหากสามารถทำได้ เนื่องจากอาจมีอาชญากรเช่น Juju Jiang

คอยจ้องมองคุณอยู่