|  |
| --- |
|  |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  | | --- | |  | | Trustworthy Computing | April 2014 | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_MS_logo.jpg | | Microsoft Security Newsletter |  | |  |  | |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  | | --- | |  | | Welcome to April’s Security Newsletter! | | Our newsletter this month focuses on guidance and tips for organizations that decide to embrace personal devices in the workplace, commonly referred to as Bring Your Own Device, or BYOD, scenarios. As [recent research](http://click.email.microsoftemail.com/?qs=e085f96b09be84d065e65feac7d2aa2183bbaf33bea8b0ba8f5ca44fa7106ecf32b4554fca209cdd) has illustrated, 78% of organizations are allowing employees to bring their own device to the office for work purposes. While the benefits such as cost savings and the adoption of newer technology are clear, BYOD scenarios can also raise important security and compliance considerations. Organizations that embrace a BYOD approach are faced with decisions such as which devices will be allowed, what kind of support will be provided, and what kind of security measures will be needed.   At Microsoft, a company with over 100,000 employees immersed in technology, embracing BYOD while continuing to meet enterprise security requirements, is a challenge. What we have learned over the years though is that having a principled approach that leverages effective standards and practices is essential to managing risk. For example, providing conditions for accessing corporate resources based on the trustworthiness of the device and identity used, can help determine the level of access provided.   In this fast moving technology market, BYOD scenarios are quickly becoming a reality for many organizations. In fact, [67% of employees in small and medium businesses indicate that they use their personal devices in the workplace](http://click.email.microsoftemail.com/?qs=e085f96b09be84d03df8fc13b6233c9f3e358d2f6a2b7befa137ee25c0df1e5e5c0e102b8175a8be) regardless of whether or not their company has practices in place. If your organization has not already embraced BYOD, are you prepared?   |  |  |  | | --- | --- | --- | | Tim Rains |  | Best regards, Tim Rains, Director Microsoft Trustworthy Computing |   Have feedback on how we can improve this newsletter? Email us at [secnlfb@microsoft.com](mailto:secnlfb@microsoft.com) and share your ideas. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Top Stories | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#SecurityGuidance) | | |  | | [The Evolving Pursuit of Privacy](http://click.email.microsoftemail.com/?qs=e085f96b09be84d067ac0b963b05605acd38ab62fccb8da83b40beec6e80e0884676da3758db6756)  As technology and our reliance on data to enable rich services continue to evolve, we must also evolve how we think about data and the ways in which societies can protect the privacy of individuals, while also allowing for responsible, beneficial data use. Explore what Scott Charney, Corporate Vice President of Trustworthy Computing, had to say on this topic and see "[We’re listening: Additional steps to protect your privacy](http://click.email.microsoftemail.com/?qs=e085f96b09be84d058c7302c049c7cee0412db40929b1af6b6c9d1c268c3478dbac7521b50800be5)" for information on some of the steps Microsoft takes to protect the privacy of its customers.   [TechNet Radio: The Risk of Running Windows XP After Support Ends](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0665bc6f48d10d43ac9a2a7b10823ded399fad223477eaa9a25cff1343c5c33c0)  In addition to his blog post entitled, "[Cyber threats to Windows XP and guidance for Small Businesses and Individual Consumers](http://click.email.microsoftemail.com/?qs=e085f96b09be84d030c70920c361d6d3a68098cdc9cfe0ca623f9290e4c80d89d251a36e603a1d3b)," Tim Rains joined the hosts of TechNet Radio's IT Time series to discuss the many security risks that end users open themselves and their organizations to by continuing to run Windows XP. Guidance and resources for those looking to migrate their business PCs to a modern operating system, like Windows 8.1 can be found on the [Windows XP End of Support](http://click.email.microsoftemail.com/?qs=e085f96b09be84d02a9e18d68a0e5d910cdc09cb5a672b2d64766f8fba9f729a68433f18efa2e5dd) page and on [TechNet](http://click.email.microsoftemail.com/?qs=e085f96b09be84d00c0234d4e1d337bb30de2bc2dff2d1caefcecf6ce7ce559f9e8004223add3efd).   [Microsoft Services Unaffected by OpenSSL "Heartbleed" Vulnerability](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0d1838ec5426574543941a2bbf7457d339569b65a1456501dfe1501f17baacc47)  On April 8, 2014, security researchers announced a flaw in the OpenSSL encryption software library used by many websites to protect customers’ data. The vulnerability, known as “Heartbleed,” could potentially allow a cyberattacker to access a website’s customer data along with traffic encryption keys. After a thorough investigation, we determined that Microsoft Services are not impacted by the OpenSSL “Heartbleed” vulnerability. In addition, Windows’ implementation of SSL/TLS was not impacted. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Security Guidance | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#CloudSecurityCorner) | | |  | | [Security Tip of the Month: Reduce Risk and Identify Vulnerabilities with the Microsoft Threat Modeling Tool 2014](http://click.email.microsoftemail.com/?qs=e085f96b09be84d053b292c87d2341e1a92f2ba2ef5d0ff567a82437d592297e7c136bd82aabb9b3)  Threat modeling is a systematic way to find design-level security and privacy weaknesses in the systems, software, and services you build and operate—for BYOD scenarios or more traditional device management scenarios. The Microsoft Threat Modeling Tool 2014 is the newest version of the free Microsoft Security Development Lifecycle (SDL) Threat Modeling Tool released back in 2011. New and improved features include:   |  |  | | --- | --- | | • | New drawing surface | |  | | | • | [STRIDE](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0731f3f57636297c27ef0dc4047512371ee41d574798fe91b2ccba3a7a79b36ce) analysis per interaction | |  | | | • | Migration for v3 threat models | |  | | | • | Updated threat definitions |   Ready to get started? Explore each of these improvements in more detail with the [Microsoft SDL Blog](http://click.email.microsoftemail.com/?qs=e085f96b09be84d053b292c87d2341e1a92f2ba2ef5d0ff567a82437d592297e7c136bd82aabb9b3), watch a [short demo](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0d655b78b9035e10879c09690d4c3aa25471abc4ad9b4e283defa6ac8b256b088), and then download [Microsoft Threat Modeling Tool 2014](http://click.email.microsoftemail.com/?qs=e085f96b09be84d05ccaeb0084a5d6c334111f75b8b808186c61ccf75ebe31595a800e22d131eda0).   [Bring Your Own Device (BYOD) Design Considerations Guide](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0b991470da0e57488076b3b8e30a35c6307e5efc57b2f1297f4f431ae572bd5ba)  Take a deep dive into the critical design considerations that need to be addressed in order to design a BYOD infrastructure that enables employees to use their own devices while protecting your company’s data. This guide covers user and device considerations, data access and protection, management scenarios, and app considerations.   [Working with Web Application Proxy](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0f65ef927cad762e45a0ee323e887751dd46ddf24165bf63847ca81d36a0f01e6)  Learn how to install and configure Web Application Proxy, a new remote access role service in Windows Server 2012 R2 that provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access them from outside the corporate network.   [Work Folders Overview](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0d567d806cff4e0ac51300f948643f510ba0cf7d1ff52b8fe0cc38c969a6ea420)  Find out how to enable users to store and access work files on personal computers and devices in addition to corporate PCs while maintaining control over corporate data.   [Manage Risk with Multi-Factor Access Control](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0916d31e5d5035e5ff8f0c5695a52544fbd87daa1c2e796c54b0064b43bb42357)  Learn how to manage risk by using Active Directory Federation Services and multiple factors for access control, including user, device, location, and authentication data.   [Join to Workplace for SSO and Seamless Second Factor Authentication Across Company Applications](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0016f9de059ef6860f328907431f2e8f7042b57250a0581941a4d1d13f62e71a6)  Find out how to utilize seamless second factor authentication and single-sign-on to provide personal devices users with secure access to workplace resources and applications.   [Managing Windows 8 Devices in a Bring Your Own Device World](http://click.email.microsoftemail.com/?qs=e085f96b09be84d02f5c6d7d0caaa8c1c9b703c7521db42b3d28287f948e0be3323f74a318eb3e6c)  Quickly see how you can manage end-user owned devices running Windows 8 with this handy checklist.   [Windows RT 8.1 in the Enterprise](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0a46f1162faf00961e60ecea0c7d55cb4f1b9d0461ba4be05b2672a41c34d27b2)  Find out how you can utilize and manage Windows RT 8.1 devices, whether employee-owned or company-owned, in an enterprise environment.   [Windows Phone 8.1 Mobile Device Management Overview](http://click.email.microsoftemail.com/?qs=e085f96b09be84d01d1ec3161e3b58ead03b46b9e494d3efc5411d0011597117040e9a91c257670d)  Download a guide to help you explore the built-in mobile device management client in Windows Phone 8.1 that lets you manage handsets with the mobile device management system of your choice. Looking to test the enterprise-grade capabilities delivered by Windows Phone 8.1—including S/MIME support and enhanced virtual private network (VPN) features—in your own environment? Get the [Windows Phone 8.1 Enterprise Preview](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0cf0a353e75c9342ac3875f082772e120ef004fcc1f808ddcb5f63169362b1d9b).   [Consumerization of IT at Microsoft: Adapting to Change](http://click.email.microsoftemail.com/?qs=e085f96b09be84d03bc725885246e16fef4968d508847814ed00057776bd49b9b308b81a0afc1618)  Learn how, to effectively manage both users’ expectations and the mandates of information security, Microsoft IT developed a programmatic approach to technology adoption—one that would foster innovation without increasing risks by introducing uncontrolled technologies. For more insight, see Microsoft Solves BYOD Using [Microsoft System Center Configuration Manager and Windows Intune](http://click.email.microsoftemail.com/?qs=e085f96b09be84d04fa01cd946f38116f86d5beeb4504e74b60ecee69a0fd7fea83ce4449d3239c0). | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Community Update | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#CloudSecurityCorner) | | |  | | New Security Baselines for Microsoft Security Compliance Manager  Two new security baselines for [Microsoft Security Compliance Manager (SCM)](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0829eac4b0786abf269cb01b26cadc5ef566b835de8b26fec34919406ed26419d), Microsoft’s popular free security and compliance tool, are now available. The first is a final, release-to manufacturing (RTM) baseline for SQL Server 2012. The second is a beta version of the baseline for Office 2013.   As with all security baselines included in Microsoft SCM, these new baselines have been created and reviewed by Microsoft security experts as well as vetted by a select group of security conscious customers as well as the Center for Internet Security (CIS). The Microsoft SCM team works closely with the CIS to ensure that both Microsoft and CIS offer clear, consistent guidance to customers on how to utilize these baselines to better secure their infrastructures.   If you are already using the latest version of Microsoft SCM, you can download the SQL Server 2012 baselines by clicking the "download Microsoft baselines automatically" link on the front page of the SCM user interface. You can also download the baseline directly:   |  |  | | --- | --- | | • | [SQL Server 2012 Baseline](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0a08e0182d4f572bf3934e1478dc41f1d9b4cc94ec663427c272d251306fe594e) | |  | | | • | [SQL Server 2012 Baseline Attachments](http://click.email.microsoftemail.com/?qs=e085f96b09be84d004421d513a3a8389f445dbdc044eda867d1916fc5d3632fa198c2a1a240eb04b) |   To get the Office 2013 Beta baseline you will need to join the Microsoft Connect program, which requires a Microsoft Account. To sign up, please visit [https://connect.microsoft.com/WindowsServer/InvitationUse.aspx?ProgramID=8455&InvitationID=8455-764K-9HVG](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0aebcdaf1f6f67d88343416d4e7f1beb4ea9cdd05bf3f22f5669e4bc594fb47a4).   The Microsoft SCM team will also be releasing security baselines for Windows 8.1, Windows Server 2012 R2, and Internet Explorer 11 in the near future. In the interim, you can access a preview of the new settings and recommendations from Microsoft by downloading the .zip package referenced at the end of the “[Security baselines for Windows 8.1, Windows Server 2012 R2 and Internet Explorer 11](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0408172c258ea310bdf3ffd70fbaf01b78cf8f46a320ade051cb88be9446f3edf)” blog post. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | This Month's Security Bulletins | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#EventsAndTraining) | | |  | | April 2014 Security Bulletins   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Critical   |  | | --- | |  | | • | MS14-017: | 2949660 | [Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0e73b406969e631c720daaeb3ff46e84b108e14374b76fe1a573f2da305b7112a) | |  | | | | | • | MS14-018: | 2950467 | [Cumulative Security Update for Internet Explorer](http://click.email.microsoftemail.com/?qs=e085f96b09be84d02e1dbf48e0dea4feddfa62bd4a5a49b9f384eb48105224e3de218dd9859a8095) |   Important   |  | | --- | |  | | • | MS14-019: | 2922229 | [Vulnerability in Windows File Handling Component Could Allow Remote Code Execution](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0ee1674d9ce3c83e344c807f44a1e10d20fd91021abacad36298da8cc7c9a4361) | |  | | | | | • | MS14-020: | 2950145 | [Vulnerability in Microsoft Publisher Could Allow Remote Code Execution](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0654bec14144416dade5533b689535fd69288a6cc9e9d3715627e581472194557) | | | |  | | April 2014 Security Bulletin Resources:   |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | • | [Microsoft Security Response Center (MSRC) Blog Post](http://click.email.microsoftemail.com/?qs=e085f96b09be84d033d3c19a0f3db3479cc3f83e1160afc58b4b513d501b602ae6c18773377ba7dd) | |  | | | • | [Security Bulletin Webcast](http://click.email.microsoftemail.com/?qs=e085f96b09be84d02202d5be7eb42ccf4b2d09f4dfa2871ce383a81aadf9448cb1300b2c1c5d8bf7) | |  | | | • | [Security Bulletin Webcast Q&A](http://click.email.microsoftemail.com/?qs=e085f96b09be84d037bde518d74734bdaa57add4691b2d24511b111b8c92496f5c41af5b2ceeb011) | | | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Security Events and Training | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#resources) | | |  | | [Microsoft Virtual Academy: What’s New in Windows 8.1 Security](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0cb403baa9caea3d5d5ada21fa2b14bbfd46519648664f4f5ee2cf890a1e8d66e)  Learn from the Windows Engineering team about the advances in security for Windows 8.1 with regard to access control, malware protection, and information protection. The course will dive into authentication and multifactor access control as well as tamper resistance hardware through UEFI, TPM, pervasive encryption, and protecting corporate data in a BYOD world.   [Microsoft Virtual Academy: Windows Server 2012 R2 Access and Information Protection](http://click.email.microsoftemail.com/?qs=e085f96b09be84d05c50f6efb56b7f3980cbb506006125779085ff441f8c1348b99dc81b3a77775d)  Learn how Windows Server 2012 R2 can help you provision, manage and secure user-owned devices while creating a seamless experience for the user.   [Microsoft Webcast: Information about the June 2014 Security Bulletin Release](http://click.email.microsoftemail.com/?qs=e085f96b09be84d032e7616c9c0aaa849521d290348a9b8a77c9c710ed73f894ed815ed74f9b94c4) Wednesday, June 11, 2014 – 11:00AM Pacific Time Join this webcast for a brief overview of the technical details of June 2014’s Microsoft security bulletins. Ask questions and get answers from Microsoft security experts.   [FastTrack Office 365 Deployments with Centrify Single Sign-on](http://click.email.microsoftemail.com/?qs=e085f96b09be84d04bc799cc4fc265bdaea1a2b9403313b13e5329a889d41e94780cd02244874ac3) Wednesday, April 30, 2014 – 11:00AM Pacific Time Explore Centrify for Office 365, a Microsoft-tested and Azure-powered solution for Active Director-based single sign-on, user provisioning and mobile management for Office 365.   [Microsoft Webcast: Information about the May 2014 Security Bulletin Release](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0cbedb68b61ff42a59d03ac907799617302341c3b08b1bb0f392796b89319f7d6) Wednesday, May 14, 2014 – 11:00AM Pacific Time Join this webcast for a brief overview of the technical details of May 2014’s Microsoft security bulletins. Ask questions and get answers from Microsoft security experts.   [Microsoft Webcast: Information about the June 2014 Security Bulletin Release](http://click.email.microsoftemail.com/?qs=e085f96b09be84d032e7616c9c0aaa849521d290348a9b8a77c9c710ed73f894ed815ed74f9b94c4) Wednesday, June 11, 2014 – 11:00AM Pacific Time Join this webcast for a brief overview of the technical details of June 2014’s Microsoft security bulletins. Ask questions and get answers from Microsoft security experts. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Essential Tools   |  |  | | --- | --- | |  | | | • | [Microsoft Security Bulletins](http://click.email.microsoftemail.com/?qs=e085f96b09be84d02d8b7ca42105b368bf39db8e1f01df147498f4708f4a89672503693090d6791d) | |  | | | • | [Microsoft Security Advisories](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0a9723d9261ca9e3ca70e9bcf3662239bafb09428860f9387c69471638fe82a30) | |  | | | • | [Security Compliance Manager](http://click.email.microsoftemail.com/?qs=e085f96b09be84d020827b28682f8dad2a03f12120ac72854818cd77794287cca3ac5fa1fdb2f576) | |  | | | • | [Microsoft Security Development Lifecycle Starter Kit](http://click.email.microsoftemail.com/?qs=e085f96b09be84d083eb556a212378b6e64829d1390d0f1202c5875ebcd9c1012ed96dcf17b89d50) | |  | | | • | [Enhanced Mitigation Experience Toolkit](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0613af374bb916a8ae353287ac397d6d9b5f39b1e60abd5d841cac20d960252a2) | |  | | | • | [Malicious Software Removal Tool](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0f48691d7a311af78a5f31b427cfedd3f71cab95c12a87dcbae4f632c229ad9b3) | |  | | | • | [Microsoft Baseline Security Analyzer](http://click.email.microsoftemail.com/?qs=e085f96b09be84d01680ab62bfe5b4a1a308bb5188d366ae2903b7de81b3bc508354730cf0da1edd) | | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Security Centers   |  |  | | --- | --- | |  | | | • | [Security TechCenter](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0bfd2e3d84abd5228eda2ff5eaf95344f9d4000da1e1b15f99910bd6269a0ef31) | |  | | | • | [Security Developer Center](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0d8d98644b703dcad338a8a219b274c05ac788828f10bf03de7fad7e5236a7c40) | |  | | | • | [Microsoft Security Response Center](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0ac1edb8069f9edd40c875aa52286323addb06c7e20101539cd4d36dc906b54c4) | |  | | | • | [Microsoft Malware Protection Center](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0b2f5ee728d3641e67a831ec71bf883874d393cf45872b337c99442df651259e1) | |  | | | • | [Microsoft Privacy](http://click.email.microsoftemail.com/?qs=e085f96b09be84d04f4c09d86d72b049cc39c460ab6393ed05aef2b30bd5a1b90462d16aa4d8ccbc) | |  | | | • | [Microsoft Security Product Solution Centers](http://click.email.microsoftemail.com/?qs=e085f96b09be84d097e7ace418332140bce2f43ddb37412bb18da5452c12cfbbed0bfeb5fe1f7325) | | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Additional Resources   |  |  | | --- | --- | |  | | | • | [Trustworthy Computing Security and Privacy Blogs](http://click.email.microsoftemail.com/?qs=e085f96b09be84d092719273d5a80f5f33560eaf476ff88c90bb1533e4269fe925f7689717e6f07d) | |  | | | • | [Microsoft Security Intelligence Report](http://click.email.microsoftemail.com/?qs=e085f96b09be84d037b706aa85545aaaeb5bfbc1d0065be2191607bc9681df92f502ab47f5402fc6) | |  | | | • | [Microsoft Security Development Lifecycle](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0cba486109478ca7acabc0f362ecc52998e6cc4a080f38832d96108202fa73707) | |  | | | • | [Malware Response Guide](http://click.email.microsoftemail.com/?qs=e085f96b09be84d032c3844630803e6f9281a68f072660ede71cff6abceb547e5c5bab47494ec197) | |  | | | • | [Security Troubleshooting and Support Resources](http://click.email.microsoftemail.com/?qs=e085f96b09be84d04aa3a0ed71dc4deeac919339748d0bc85b04880e9ffe74672291186f990d5bdb) | |  | | | • | [Trustworthy Computing Careers](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0ebda7540952f4e1b69c47c2d4b1c402d6dad87eca685549ab22d57211b121b5f) | | | | |  | |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | |  | microsoft.com/about/twc | Trustworthy Computing |  | |  |  |  |  | | | |  | | --- | |  | |  | This is a monthly newsletter for IT professionals and developers–bringing security news, guidance, updates, and community resources directly to your inbox. If you would like to receive less technical security news, guidance, and updates, please subscribe to the Microsoft Security for Home Computer Users Newsletter.   © 2014 Microsoft Corporation [Terms of Use](http://click.email.microsoftemail.com/?qs=e085f96b09be84d001deac79ca924adb15ddd1bad4e3298bbf8a39a00a49059ce7e4fe605396c435) | [Trademarks](http://click.email.microsoftemail.com/?qs=e085f96b09be84d05f605d30ed5a40197b690e64314d1d96c83788fdf250d30e5445e6522b805074)   Microsoft respects your privacy. To learn more please read our online [Privacy Statement](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0e0334b51665bb1d15f34a64ec1a437514d54b3608894f3a522f56d2519d85473).   If you would prefer to no longer receive this newsletter, please [click here](http://click.email.microsoftemail.com/?qs=e085f96b09be84d0707f808791a2ae0ec0a97e9161e9b54c9deba0097f4e75d634d7a2d3196d950f).   To set your contact preferences for other Microsoft communications [click here](http://click.email.microsoftemail.com/m_hcp.aspx?qs=0bb7f39debca1b0acb34d76711c30a6a96abb33fd8cde0008d7a64657972b3f57ed47edd117f26836cc535108b4fcce9bc5b1bb45d9f9373192536d2b1fa2efd1b7d1a2ee9877fd73b4438c7e4328bf6fdd879c6505f876d9c17aec181697ba2c58593c3ca7a3ed2).   Microsoft Corporation One Microsoft Way Redmond, WA 98052 USA | |  | |  |  |  |  | | |  | | |