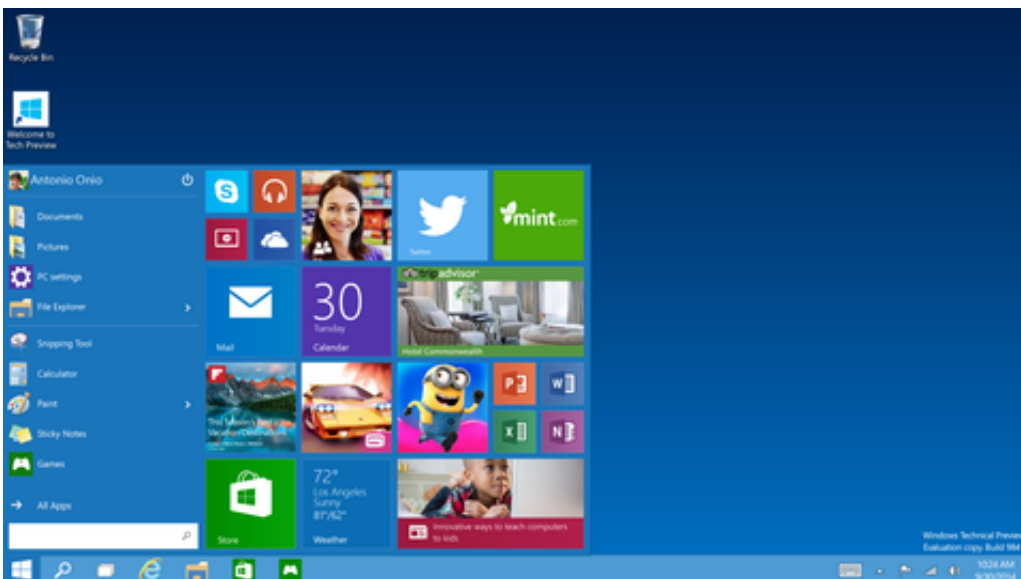# Microsoft beefs up security protection in Windows 10

October 25 2014, by Nancy Owano

What Microsoft users in business care deeply about—-a system architecture that supports efforts to get their work done efficiently; a work-centric menu to quickly access projects rather than weather readings and movie trailers; and an architecture that helps protect their identity and information. Small wonder that Microsoft is talking up the security feature of its next-generation Windows 10 operating system. Its security measures are impressive in delivering two-factor authentication and other safeguards against malware and data theft.

The posting from Jim Alkove, leader, Windows enterprise program management team, stated that Windows 10 security "represents the destination in our journey to eliminate the use of single-factor identity options like passwords. We believe this solution brings identity protection to a new level as it takes multi-factor security which today is limited to solutions such as smartcards and builds it right into the operating system and device itself." Announcements about the security side of Windows 10 were also posted in the company's corporate blog, The Fire Hose. The news via The Fire Hose is that the latest preview release has nearly everything in place to move away from single-factor authentication options such as passwords. Once enrolled, devices themselves become one of two factors that are required for authentication. The second factor will be a PIN or biometric, such as fingerprint.

"From a security standpoint, this means that an attacker would need to have a user's physical device – in addition to the means to use the user's credential – which would require access to the users PIN or biometric information," said Alkove. Smartphones can be used as a mobile credential. Alkove said, "Users will be able to enroll each of their devices with these new credentials, or they can enroll a single device, such as a mobile phone, which will effectively become their mobile credential. It will enable them to sign-in into all of their PCs, networks, and web services as long as their mobile phone is nearby. In this case, the phone, using Bluetooth or Wi-Fi communication, will behave like a remote smartcard and it will offer two factor authentication for both local sign-in and remote access."

As for malware, the Fire Hose blog notice said a range of options has been included to help businesses protect against common causes of malware infection. What's more, said the blog, Windows 10 "renders phishing attacks for identities almost completely ineffective."

Alkove noted that cyber-attacks on businesses are not only wide-reaching but increasingly high-profile and successful in execution. "In a couple of recent cases, hackers infiltrated Fortune 500 companies using stolen usernames and passwords which gave them access to point of sale systems and the credit card data being processed with them. The attacks resulted in the theft of millions of credit card numbers which quickly ended up in the black market." Windows 10's architects clearly felt they had to mean business: security features include automatic encryption of corporate apps, data, email, website content and other sensitive information. Windows 10 provides organizations with the ability to lock down devices, said Alkove. "Because malware is often inadvertently installed onto devices by users, Windows 10 addresses this threat by only allowing trusted apps, meaning apps that are signed using a Microsoft provided signing service, to be run on specially configured devices." He said organizations will have the flexibility to choose what apps are trustworthy – "just apps that are signed by themselves, specially signed apps from ISVs, apps from the Windows Store, or all of the above."

More information: — blogs.microsoft.com/firehose/2 … d-security-measures/

— blogs.windows.com/business/201 … or-the-modern-world/

© 2014 Tech Xplore