ENTRUST
TECHNOLOGY CONSULTING SERVICES

Highlights from ENTRUST's IT Panel Discussion:

Microsoft Myths Exposed & More

By Mitchell R. Sowards

Introduction from Mitch

ENTRUST offers customer events every quarter called "New Technology Showcases." Last month, there did not happen to be any new products that we wished to showcase, so instead we offered our customers a Panel of Technology Experts to answer all kinds of questions.

Due to the popularity & positive response we received from our audience, we plan to host similar events in the future. We encourage you to attend our future panel discussions, so be sure to look for more information coming soon.

In the meantime, I've included Highlights from our event in this whitepaper for those who were not able to attend. However, it wasn't possible to include all of the questions and answers, so we'll be hosting a follow-up event:

***LIVE* Virtual Q&A Session with Mitch**
Where: LIVE on Facebook
When: Friday, June 22
Time: 12 pm to 1pm

To Participate: Go to our Facebook Page, LIKE our Post, and Post your questions or comments. Check back in **Friday at Noon** for the Live Q&A Session with me.

Meet the Panelists

MITCH SOWARDS (myself)
ENTRUST Consulting Services Manager

CLAY PRICE
ENTRUST Senior Engineer and Chief Investigator for ENTRUST Labs

LARRY FOOTE
Microsoft Partner Territory Manager (Texas, Oklahoma, Louisiana & Arkansas)

MICHAEL ESPINOZA
Owner, Technology Coaching, a local firm specializing in mobile technology and providing one-on-one technology coaching/training for busy executives and business owners.

TONY ALARCON (Emcee)
ENTRUST Sales and Marketing Manager

Event Highlights

CATEGORY: SECURITY

QUESTION: Can I really get a VIRUS or "get hacked" just by *visiting* a website?

ANSWER: YES! In fact, *the most common vector for malware infections today is through web browsing!* When you visit a website, there are animations occurring. When you move your mouse across the screen you may notice that the parts of the screen you are traversing change (for example, ads may "pop up"). All of those things are computer code being downloaded to your PC to make the animations occur. If you are lured to a malicious website, it will be full of these things and each of them will attack your computer. Your antivirus software will try to protect you but no protection is perfect. Even legitimate websites are "composites" of content from multiple locations. For example, when you visit CNN.com for news, ads come from somewhere else. So, if one of those advertisers gets compromised, you could get a virus from a legitimate site.

BEST PRACTICE: ① Try to visit only legitimate websites and steer clear of unknown sites. ② Look for "Protected by…" seals. Many legitimate sites pay antivirus vendors, like McAfee or Symantec to regularly scan their website to make sure no malware has penetrated them.

QUESTION (from the audience)**:** What about email? If I receive an email with fancy graphics (HTML) can I get a virus even if I only view it in my Outlook preview pane?

ANSWER: ① YES, because the Outlook preview pane is essentially downloading "active" content from the internet to display to you. Infected content can attack your machine through the preview pane. ② If you have doubts about an email, try opening it on your smartphone first/instead to check it out. While there are a growing number of malware targeting mobile devices (over 3000 in 2012 already), most malware targets only PCs (or Macs). So, if you read the email on your phone you have an opportunity to delete it before it can attack your PC.

ENTRUST™
TECHNOLOGY CONSULTING SERVICES

CATEGORY: SECURITY

QUESTION: How can I block my employees from visiting specific sites like Facebook?

ANSWER: With a modern firewall we can block Facebook for the casual user. Sophisticated users (like "geek teenagers") will know ways to get around that, so you would need a more sophisticated tool that does web content filtering. If you really, really want to absolutely block Facebook (and similar sites) it requires even more sophisticated and expensive web content filtering tools.

BEST PRACTICE Have a written POLICY that states that you expect employees not to waste time on Facebook using company computers. In that policy, encourage employees to use their own devices (smartphones, tablets/iPads, etc.) for those activities only during legitimate personal time, like lunch breaks. Since most employees have such devices these days, they likely will comply. Then you can implement the less expensive two forms of blocking (firewall and basic web filter). Even sophisticated teenager/geeks will then find it easier to use their own devices rather than try to sneak past company blocking mechanisms.

QUESTION: What's the best kind of password to have? How long? How complex? How often should it be changed?

ANSWER: The best kind of password is a LONG ONE even without complexity (minimum 12-16 characters). A long password without complexity is virtually unbreakable while a short password, even with complex combinations of lowercase and uppercase letters, numbers, and special characters is easily cracked with modern hacking tools. ENTRUST Labs' recommendation is to use a "passphrase" that is long but easy to remember like: "myfavoritefoodispizza" which is 21 characters long. If you add complexity it's even harder to crack but without being much harder to remember: MyFavoriteFoodIsPizza. Feel free to use bible passages or inspiring quotes – anything that is easy to remember will work.

BEST PRACTICE Change your PC password every 90 days or as often as you can tolerate. For many organizations this will be driven by how often you can get the VIPs (President, Partners, Owners) to change their password. If you can't get the VIPs to change every 90 days, then at least go for twice per year (180 days).

ENTRUST™
TECHNOLOGY CONSULTING SERVICES

CATEGORY: LICENSING/SOFTWARE

QUESTION: Does Microsoft ever have "sales" or "promotions" when buyers can save money?

ANSWER: If you are purchasing "retail" products (such as at a big box store) they will have periodic sales. But if your organization purchases software directly from Microsoft through one of their licensing programs, YES Microsoft has regular promotions when you can purchase products at discounted prices or get rebates.

BEST PRACTICE Visit www.microsoftincentives.com for all current Microsoft promotions. Microsoft's incentive programs change every few months, so be sure to check in regularly.

QUESTION: What's the best way to purchase Microsoft Office software?

ANSWER: It depends. The cheapest way is to purchase it pre-installed on a new computer (called "OEM" software) and if you only have 2-5 computers that might make sense. But there are some drawbacks for larger customers. Purchasing OEM software leads to different users having different versions as the years go by. Also, OEM software is forever tied to the original machine. So, if a computer dies after a year and you want to replace it, you have to buy the Microsoft software again. For larger customers, the best way to purchase Microsoft Office is directly from Microsoft on one of their "Open Licensing" programs. Unfortunately to meet the needs of the smallest customers up to the largest, Microsoft has multiple licensing programs and their ins-and-outs can be very complex.

BEST PRACTICE Work with ENTRUST to identify the best licensing program for your company. In general we find that purchasing software on Microsoft's 3-year, Open Value plan using their interest-free "split-pay" plan is the best combination of value and cost. This plan includes "Software Assurance" that (among other benefits) allows you to keep all users on the same version all the time (with free upgrades) and allows users to download a copy of the SAME version on their home PCs (so they can work for you at home) for only $10.

ENTRUST
TECHNOLOGY CONSULTING SERVICES

CATEGORY: MOBILITY & SECURITY

QUESTION: It's a pain to keep track of all my passwords. What do you think about "password vault" programs?

ANSWER: Password vault programs are a great way to securely keep track all of your passwords.

> **BEST PRACTICE** Michael currently recommends 1Password from a company named AgileBits. He likes it because it runs on multiple platforms (Mac, PC, iPad/Pod, etc). Visit www.agilebits.com or download/purchase through your mobile device's appstore or iTunes.
> **CAVEAT:** 1Password stores all of your passwords in "the cloud" and synchronizes the vault among all of your many devices to make it easy to access from any device. This is very convenient. And, of course, all of your information in "the cloud" is encrypted and protected. BUT if your master 1Password password is ever compromised, then your vault becomes accessible to the thief from anywhere even if they don't have access to one of your devices.

CATEGORY: HARDWARE

QUESTION: How often should I replace my PCs or SERVERS?

ANSWER: Replace both PCs and Servers after 3-5 years. If your needs or software don't change very often (and thus does not require more speed and capacity), then you might be able to make a PC or Server last 5 years. If your needs change or you are constantly upgrading the software you use, maybe you will find PCs and Servers being too slow or too full after only 3 years. If a PC or server makes it to the 4 year mark, you should start planning for its replacement and decide exactly when in the next 12 months it can be retired or at least "passed down" to a role with lower needs.

> **BEST PRACTICE** For SERVERS, be careful about allowing a server that is "working fine" to go beyond 5 years. After 5 years, most hardware manufacturers (Dell, IBM, HP, etc.) stop offering service contracts. You don't want to be in a situation where your server crashes and ENTRUST has to scramble around, perhaps for days, trying to repair it. For NOTEBOOKS/LAPTOPS the 3-5 year rule is reduced to 2-4 years because these devices take a lot of wear-and-tear and don't last as long. They typically are less powerful than desktops of the same age and so they "run out of juice" sooner.

Learn more about ENTRUST: www.entrust.us.com
Contact us at: info@entrust.us.com
Call us at: 866-863-4738