

### News Article

## Steve Jobs' Death Launches Online Attacks

On October 5th 2011, the world lost a visionary and a creative genius with the death of Apple co-founder Steve Jobs. Jobs, who died aged 56, left legions of Apple fans and technical industry advocates scouring the Internet for news of his death. As with any newsworthy item, cybercriminals quickly took full advantage of users' natural curiosity and gullibility and launched several Facebook scams.

### Free iPad giveaway hoax

Within hours of the official announcement of Jobs' death, cybercriminals used Facebook to spread claims that Apple was giving away free iPads 'in memory of Steve Jobs'. This scam asked users to share the link to a page in order to become eligible to claim the device. It also instructed users to enter some text in the comment box below the Share link. However, following the instructions only redirected users to several ad sites and automatically reposted the malicious link on their Walls as spam. Of course, no such iPad offer existed, but many users may have fallen for the ruse.



The next Facebook or email link you click may be a portal into the lair of spies and thieves

### Steve Jobs alive! Spam run

Albeit using a different lure, we found spam bearing the subject, "Steve Jobs Alive!" The email message's body contained a link that led to a site that appears to be blank, which may not even be so. It can, for instance, contain an invisible iframe that can redirect users to malicious sites or can lead to the download of malware that can harm their systems. The scam, while tasteless, is not new in terms of approach, but we will continue to be on the lookout for further developments.

### New threats and new vigor

The recent attacks related to Steve Jobs' death shows the renewed vigor with which cybercriminals utilize social engineering. Almost every major holiday, event, or news item will be used for malicious purposes. Steve Jobs' passing is no exception.

### Be safe – not sorry

To stay protected all the time, follow these online safety tips:

- When connecting to a wireless network, be careful sending messages you don't want to land on the bad guys' laps.
- Be wary of the email you receive, some malicious messages are designed to look real.
- Always check URLs prior to clicking. Though not foolproof, it is useful to check if its URL starts with https.
- Update security solutions and all other applications. To keep your system protected from threats like viruses, spyware, Trojans, hacking tools, and other malware, keep your patch levels up to date.

November 2011

Page 1

Articles in This Issue...

News:

Steve Jobs' Death Launches Online Attacks

Tips for the Office:

Microsoft ships final Office 2007 Service Packs

Did You Know:

4 Steps to Stop Data Loss

Question of the Month:

Can I clean my monitor with Windex?

Quote of the Month

Product of the Month:

Dell Latitude XT3 Tablet PC

November 2011

Page 2

Articles in This  
Issue...

**News:**

Steve Jobs' Death  
Launches Online  
Attacks

..... 1

**Tips for the Office:**

Microsoft ships final  
Office 2007 Service  
Packs

..... 2

**Did You Know:**

4 Steps to Stop Data  
Loss

..... 3

**Question of the Month:**

Can I clean my monitor  
with Windex?

..... 4

**Quote of the Month**

..... 4

**Product of the Month:**

Dell Latitude XT3 Tablet  
PC

..... 5

## Tips for the Office



### Microsoft Ships Final Office 2007 Service Pack

Source: Computerworld



Microsoft on Tuesday delivered its last service pack for Office 2007.

Service Pack 3 (SP3), which weighs in at 351MB, was posted to Microsoft's download center and has begun appearing as an optional install through Windows Update.

Microsoft won't start automatically downloading and installing Office 2007 SP3 onto customers' PCs for 90 days.

SP3 is Office's 2007's first service pack since 2009's SP2, and with the upcoming end of mainstream support, almost certainly its last.

The service pack's debut was not a surprise: Earlier this month, Microsoft promised to ship the update this month.

Microsoft was under a self-imposed deadline to get SP3 out in October because it wanted to give enterprise customers six months to test and deploy before the suite is retired from mainstream support on April 10, 2012.

Once Office 2007 exits mainstream support, Microsoft will supply most customers security updates only during a five-year extended support phrase that runs through April 11, 2017.

Users can continue to run Office 2007 SP2 -- that edition doesn't stop working -- but Microsoft will halt all security updates to SP2 a year from now.

Links to the download pages for the various permutations of Office 2007 SP3 can be found in this Microsoft blog post .

Office 2007 went on general sale in January 2007 alongside Windows Vista, but was supplanted by Office 2010 more than a year ago.

November 2011

Page 3

Articles in This Issue...

### News:

Steve Jobs' Death Launches Online Attacks

..... 1

### Tips for the Office:

Microsoft ships final Office 2007 Service Packs

..... 2

### Did You Know:

4 Steps to Stop Data Loss

..... 3

### Question of the Month:

Can I clean my monitor with Windex?

..... 4

### Quote of the Month

..... 4

### Product of the Month:

Dell Latitude XT3 Tablet PC

..... 5

## Did your know...

### 4 Steps to Stop Data Loss from Your Small Business

If you've ever wondered who has the time and money to worry over security issues when they've got a small business to run, you're not alone. Many small business owners overlook even basic computer security. Not surprisingly, cybercriminals have been exploiting small and medium-sized businesses with ease and great success.

Consider the following scenarios: **customer credit card information is accidentally sent to someone outside the company, an email containing profanity is sent to someone outside the company, A cashier downloads transaction details to an iPhone via the USB port on a retail POS (Point Of Sale) computer, Employees use personal web mail accounts to send confidential company information.**

Any of these situations could lead to an internally originated security breach. Avoiding such a breach through data loss protection (DLP) might sound like an expensive solution that only large companies can afford but, if you do your research up front, you might be surprised at what you can accomplish quickly and easily without spending a fortune.

#### Step 1: Define What Data is Sensitive

Take a careful inventory of your data and determine how much of it you actually need to worry about. Some examples of confidential data include: **Credit cards/store cards, Contracts and quotes, Customer contact details, Finance & accounting files, HR or health-related information, Intellectual property, Confidential business projects.**

Look for DLP solutions that come with pre-set definitions and give you the flexibility to add and change definitions for confidentiality.

#### Step 2: Identify Content to be Monitored or Quarantined

Email is one obvious example of content that should be monitored. Anyone, including trustworthy employees with good intentions, could make an honest mistake and accidentally email confidential data to the wrong person. A malicious user could do far worse—emailing profanities, racial comments, or adult materials, not to mention company secrets or confidential customer information. You want a DLP solution that can detect malicious users' attempts to disguise confidential files by re-naming, copy-and-paste, or other methods.

#### Step 3: Identify Common Leak Points

Email should be the first place to look for data leaks because it's a primary means of communication these days—and because it has so often been the source for data leaks before. Another increasingly common leak point these days is USB ports. Everything in this list is essentially a mobile storage device: **Digital cameras, iPods and other digital music players, Smartphones and tablet computers, Ebook readers, USB thumb drives, Mobile data storage devices**

#### Step 4: Find an Affordable Solution

DLP is no longer a luxury affordable only by large organizations, nor is it a time-consuming exercise that takes months to implement. Trend Micro provides a solution for small and medium businesses to prevent data loss through email and USB ports: Worry-Free™ Business Security – Advanced.

Technology is improving data accessibility even as security threats grow. In today's environment, security should not be just a defense strategy against external threats—it should also deliver proactive protection against data loss from internal sources. Regardless of the size of your company, a sound security approach that extends security to cover key data leak points will save you unforeseen problems and costs.

November 2011

Page 4

Articles in This  
Issue...

News:

Steve Jobs' Death  
Launches Online  
Attacks

Tips for the Office:

Microsoft ships final  
Office 2007 Service  
Packs

Did You Know:

4 Steps to Stop Data  
Loss

Question of the Month:

Can I clean my monitor  
with Windex?

Quote of the Month

Product of the Month:

Dell Latitude XT3 Tablet  
PC

## Question of the Month



**Question:** Can I clean my computer monitor with Windex?

**Answer:** It is not okay to spray Windex (or anything else) on a monitor. In fact, when it comes to cleaning an LCD screen, there's a right way and a wrong way. Let's focus on the right way. For starters, turn your monitor off. There will be some moisture involved in this cleaning, and the last thing you want is for liquid to come into contact with anything powered.

Next, find a clean, soft cloth (a paper towel will do, but it's far from the best choice), then dampen it with water. Don't soak it--there should be no dripping to speak of--just get it moist. And don't use anything other than water. Ammonia- and alcohol-based cleaners can ruin an LCD. If your screen is seriously gunked up, and plain water doesn't get the job done, you can use a 50/50 solution of distilled water and white vinegar.

Finally, let the screen air-dry for a few minutes, or gently wipe it dry with a fresh cloth. When you're absolutely certain it's 100 percent dry, plug it back in and turn it on.



**"You forgot to respond to the e-mail I meant to send!"**

## Quote of the Month

**Innovation distinguishes between a leader and a follower.**

Steve Jobs

## Product of the Month

### Dell Latitude XT3 Tablet PC

#### Get the flexibility of a tablet with the power of a laptop

Have it all: the convenience of a touch-screen tablet, the power of an enterprise-grade laptop and a large display. Whether at your desk or on the move, the Latitude™ XT3 lets you work almost anywhere.

- **High light, low light or no light:** Stay productive in the office or in the field with a large, 13.3" auto-bright HD display and backlit keyboard option.
- **No compromises:** Get the mobility and flexibility of a tablet without sacrificing the power of an enterprise-class laptop.
- **Easy integration:** Use your existing Latitude E-Family docking stations, power adapters, media modules and extended battery slice.

#### The screen that's also the perfect workspace

Whether you're working indoors or outside, the Latitude XT3 offers an ideal balance between usable workspace and mobility. Multiple input options, wide viewing angles and a large multi-touch screen enable you to work where and how you like.

- **Picture-perfect clarity:** View your work in stunning detail with the 13.3" HD LCD.
- **Right in any light:** Enjoy easy viewing in sunlight with the optional outdoor-viewing screen.
- **Let your fingers do the work:** Enjoy maximum usability with four-finger touch control, touchpad, trackstick and mouse input capabilities.



#### The tablet that keeps up with your busy day

Who says you have to choose between performance and mobility? With the Latitude XT3, you get the power, connectivity and security of an enterprise-class laptop with easy conversion to tablet mode.

- **Speed and connectivity** Power through your day with the speed of Intel® Core™ i3, i5 or i7 processors, Genuine Windows® 7 Professional and connectivity options that include WiMAX™ and mobile broadband.
- **All-day battery capacity** Your unpredictable day demands flexible power options. Latitude XT3 offers 3 - and 6-cell Express Charge™ battery options with a 9 -cell extended battery and slice option for all day power.<sup>1</sup>
- **Advanced security** Your Latitude XT3 offers Dell data protection that can encrypt data and help guard against unauthorized access.



November 2011

Page 5

Articles in This Issue...

#### News:

Steve Jobs' Death Launches Online Attacks

1

#### Tips for the Office:

Microsoft ships final Office 2007 Service Packs

2

#### Did You Know:

4 Steps to Stop Data Loss

3

#### Question of the Month:

Can I clean my monitor with Windex?

4

#### Quote of the Month

4

#### Product of the Month:

Dell Latitude XT3 Tablet PC

5