

News Article

What the Mayan Calendar Doesn't Predict: Threats in 2012

With 2012 beginning, it's time once again to look to what awaits us in the ever-changing online threat landscape. From the way businesses allow employees to use personal gadgets at work, to what sort of malware may be in the offing, discover what may come our way in the Mayan calendar's most ominous year yet.



Consumerization to increase

In a recent Trend Micro report 74% of the survey respondents said they readily took part in consumerization. A healthy majority of end users preferred to use their own devices specifically because of ease of use, convenience. This means companies may be forced to deal with security and data breaches next year. A study revealed that 50% of IT decision makers agree in providing full support for employee-owned devices and 79% also said employees would be required to install mobile security solutions on their own devices.

Conventional attacks to remain effective

While virtual machines (VMs) and cloud computing services can very well herald a new type of specialized attack, conventional targeted attacks will remain effective in new environments. Virtual and cloud platforms, as detailed in a recent Trend Micro report, are just as vulnerable as physical platforms, and even more difficult to protect. IT administrators will have to take extraordinary measures to secure their company's critical data with the adoption of these new technologies.

Mobile malware to rise

Most smartphone and tablet platforms will be targeted by more and more cybercriminal attacks. The Android OS, in particular, has become a very popular target due to the way in which Android app stores work. Major security vulnerabilities will be found among legitimate mobile apps, which can spell easier access to user data for cybercriminals.

Botnets to shrink - and grow...

Though botnets may be smaller in size in order to evade detection, these will grow in number. In 2011, several botnet takedowns took place with notable examples including the Esthost, Mariposa, Rustock, and CoreFlood. Non-traditional targets like those targeted by STUXNET may also come under more attacks next year.

Breaches to increase

2011 saw an alarming number of data breaches. The most notable incidents involved hacker groups - Anonymous and LulzSec and it's still reasonable to believe they will become more prevalent next year.

Next-generation privacy

Social networking has changed what online privacy means. And this trend will continue in 2012 as users no longer mask real names, hide personal photos, and reveal their locations. This will make it easier for cybercriminals to steal information and to possibly enact more damaging identity theft attacks.

More targeted attacks on smaller scale

Targeted attacks will no longer just target large enterprises. Small and medium-sized businesses will become fair game as well. Highly targeted attacks against organizations relied on personal and confidential corporate information inadvertently leaked via social networking sites; this will no doubt continue to be the case next year.

New threat actors will emerge

In 2012, new threat actors using new and more sophisticated tools will also emerge. This will lead to more high-profile attacks, involving the theft of critical company information via malware infection and hacking.

February 2012

Page 1

Articles in This Issue...

News:

What the Mayan Calendar Doesn't Predict: Threats in 2012

..... 1

Tips for the Office:

Outlook 2007: Print a Blank Calendar

..... 2

Did You Know:

How to Lock Down your Wireless Network

..... 3

Question of the Month:

How do I merge cells in Excel?

..... 4

Quote of the Month

..... 4

Product of the Month:

Parallels Desktop 7

..... 5

February 2012

Page 2

Articles in This
Issue...

News:

What the Mayan
Calendar Doesn't
Predict: Threats in 2012

Tips for the Office:

Outlook 2007: Print a
Blank Calendar

Did You Know:

How to Lock Down
your Wireless Network

Question of the Month:

How do I merge cells in
Excel?

Quote of the Month

Product of the Month:

Parallels Desktop 7

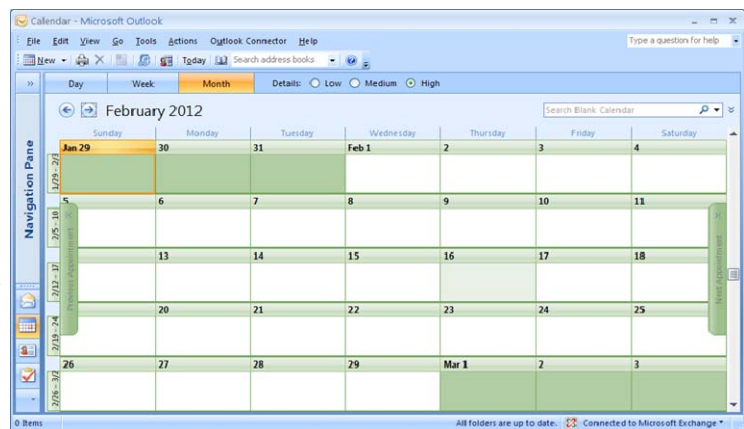
Tips for the Office



Outlook 2007: Print a Blank Calendar

Sometimes you need a hard copy of a calendar to use for various planning tasks. If you don't want your appointments listed on the calendar, you can print a blank calendar by following these steps:

1. Go to the menu, click **File**, mouseover **New** and select **Folder** (or you can use the keyboard combination **Ctrl+Shift+E**).
2. In the Create New Folder window, input a name for the new Calendar in the first textbox.
3. From the **Folder contains** dropdown, select **Calendar Items**.
4. Use the bottom section to select the location you wish to place the newly created Calendar.
5. Click OK.
6. Go to the Calendar view in Outlook.
7. Under **My Calendars** in the left pane, select the checkbox next to the newly created calendar.
8. Go to the Menu, click **File** and select **Print** (or use the keyboard combination **Ctrl+P**).
9. In the **Print** window, use the **Print this calendar** dropdown to select the newly created calendar.
10. Use the **Print style** section to select the style you wish to use when printing the calendar.
11. Input the **Start** and **End** dates in the **Print range** section.
12. Click the OK button to print the blank calendar.



Don't delete your new calendar so that the next time you need a blank calendar, you just have to select it, add the date range and print style and it's ready to go.

Did your know...

How to Lock Down Your Wireless Network

Source: Alex Wawro, PCWorld

If you operate a wireless network for your home or business, it's important to protect it against opportunistic hackers seeking to steal your data or hijack your Wi-Fi for their own nefarious purposes. We spoke to Steven Andrés, CTO of security consulting firm Special Ops Security, to learn about the best ways to lock down your Wi-Fi. To get started, you'll need to log in to your router's administrative console by typing the router's IP address into your Web browser's address bar. Most routers use a common address like 192.168.1.1, but alternatives like 192.168.0.1 and 192.168.2.1 are also common. Check the manual that came with your router to determine the correct IP address; if you've lost your manual, you can usually find the appropriate IP address on the manufacturer's website.



Change Your Passwords

The first step in securing your network is simple: Change your passwords! Default router passwords like "admin" are seductively simple to remember, but that means they're equally simple for a hacker to guess; there's even a public database containing default login credentials for more than 450 networking equipment vendors. Though no password is foolproof, you can build a better password by combining numbers and letters into a complex and unique string. Remember to change both your Wi-Fi password (the string that guests enter to

access your network) and your router administrator password (the one you enter to log in to the administration console--the two may sometimes be the same).

Change Your SSID

Every wireless network has a name, known as a Service Set ID (or SSID). The simple act of changing that name discourages serial hackers from targeting you, because wireless networks with default names like "linksys" are likelier to lack custom passwords or encryption, and thus tend to attract opportunistic hackers. Don't bother disabling SSID broadcasting; you might be able to ward off casual Wi-Fi leeches that way, but any hacker with a wireless spectrum scanner can find your SSID by listening in as your devices communicate with your router.

Enable WPA2 Encryption

If possible, always encrypt your network traffic using WPA2 encryption, which offers better security than the older WEP and WPA technologies. Every device that accesses the Internet has a Media Access Control (MAC) address, which is a unique identifier composed of six pairs of alphanumeric characters. You can limit your network to only accept specific devices by turning on MAC filtering, which is also a great tip for optimizing your wireless network.

Limit DHCP Leases to Your Devices

Dynamic Host Configuration Protocol (DHCP) makes it easy for your network to manage how many devices can connect to your Wi-Fi network at any given time, by limiting the number of IP addresses your router can assign to devices on your network. Tally how many Wi-Fi-capable devices you have in your home; then find the DHCP settings page in your router administrator console, and update the number of "client leases" available to the number of devices you own, plus one for guests. Reset your router, and you're good to go.

Finally, enable the Block WAN Requests option, to conceal your network from other Internet users. With this feature enabled, your router will not respond to IP requests by remote users, preventing them from gleaning potentially useful information about your network.

February 2012

Page 3

Articles in This Issue...

News:

What the Mayan Calendar Doesn't Predict: Threats in 2012

1

Tips for the Office:

Outlook 2007: Print a Blank Calendar

2

Did You Know:

How to Lock Down your Wireless Network

3

Question of the Month:

How do I merge cells in Excel?

4

Quote of the Month

4

Product of the Month:

Parallels Desktop 7

5

February 2012

Page 4

Articles in This
Issue...

News:

What the Mayan
Calendar Doesn't
Predict: Threats in 2012

1

Tips for the Office:

Outlook 2007: Print a
Blank Calendar

2

Did You Know:

How to Lock Down
your Wireless Network

3

Question of the Month:

How do I merge cells in
Excel?

4

Quote of the Month

4

Product of the Month:

Parallels Desktop 7

5

Question of the Month

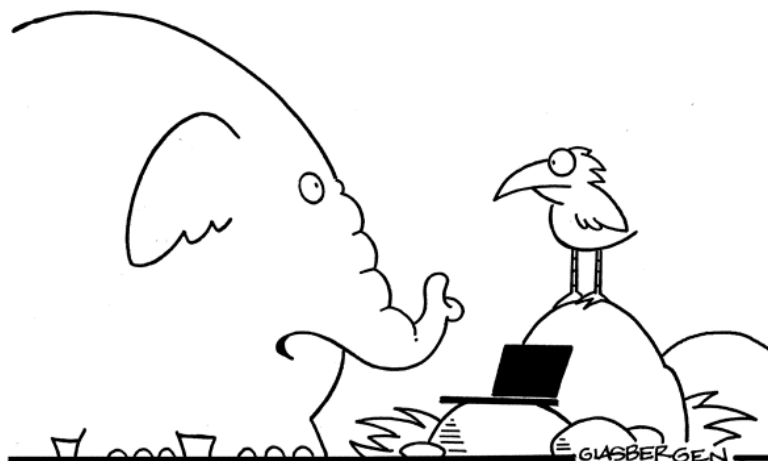


Question: How do I merge cells in excel?

Answer: Spreadsheets allow users to merge and split cells. The "Merge Cells" option in Microsoft Excel provides a helpful tool for data formatting. By merging the contents of multiple cells, users can center data across multiple columns to create spreadsheets that are easy to read. Sometimes it is necessary to split previously merged cells. A few quick clicks returns any merged cell to its original format. Review these steps and remember them for easily splitting a merged cell.

Instructions:

1. Right click on the merged cell. Click "Format Cells."
2. Click on the "Alignment" tab.
3. Uncheck the "Merge Cells" check box by clicking on it.
4. Click "OK". The merged cells are now split.
5. Click on the icon for merged cells on the menu bar if available to enable or disable merged cells when needing a quick shortcut.



"They say an elephant never forgets, but that was before I had so many passwords, user names and PIN numbers!"

Quote of the Month

Without ambition, no conquests are made, no lands discovered, no business created.

Ambition is the root of all achievement.

- James Champy

Product of the Month

Parallels Desktop 7

Run Windows on your Mac

Discover Parallels Desktop for Mac

Parallels Desktop for Mac is the most tested, trusted and talked-about solution for running Windows applications on your Mac.

Seamless Simplicity

With Parallels Desktop for Mac, you can seamlessly run both Windows and Mac OS X Lion applications side-by-side with speed, control and confidence.

Innovation

Setting up Parallels Desktop for Mac is easy. Bring all your PC programs, documents, photos, music and browser bookmarks to your Mac, then run them all like they were made for your Mac. It's the best of both worlds on one desktop — without rebooting.

Performance and Personalization

Experience as much or as little Windows as you want. Multiple view modes make it possible for you to customize the level of integration between Mac and Windows without compromising performance.



February 2012

Page 5

Articles in This Issue...

News:

What the Mayan Calendar Doesn't Predict: Threats in 2012

..... 1

Tips for the Office:

Outlook 2007: Print a Blank Calendar

..... 2

Did You Know:

How to Lock Down your Wireless Network

..... 3

Question of the Month:

How do I merge cells in Excel?

..... 4

Quote of the Month

..... 4

Product of the Month:

Parallels Desktop 7

..... 5