



Information Communications Technology Newsletter

11th October 2007

Foundation for Information Technology Accessibility
Improving the quality of life of disabled persons through ICT.

Contents

Welcome to the 45th issue of the FITA newsletter. We welcome your contributions. Email us on stanley.debono@gov.mt or michael.micallef@gov.mt.

- Software of the month
- Website of the month
- Question Box
- Articles
- Credits
- Disclaimer
- MS Accessibility CD
- The low-cost laptop
- Help keep spam out of your inbox
 - Pump-and-dump scams
 - 11 tips for safer instant messaging
 - How to use social networking Web sites more safely
 - How to tell fact from opinion on the Internet
 - RATs and how to help avoid them
- 'Pay By Touch' Bank Cards Launched In London
- Braille Translations
- Free EASI resources
- YouTube SPAM
- Excel 2007 calculation bug

Software of the month

++ MS Accessibility CD

Do you have someone at your office or do any of your clients have anyone that could benefit from additional accessibility on their computer, such as making the computers more comfortable to see, hear and use? If so, you may want to take advantage of the Free Microsoft Accessibility CDs offer from Microsoft that provides accessibility demos and tutorials for Windows Vista, Windows XP, Internet Explorer 6 and 7, and more accessibility resources. The best part, this resource is free to you and your clients. Head over to the Free Microsoft Accessibility CD order page and get one today.

<http://www.microsoft.com/enable/cd/default.aspx>

Contributed by: Mr. Eric Ligman

Website of the month

++ The low-cost laptop

The buzz around the XO Laptop, aka the One Laptop Per Child group's "\$100 laptop" is growing, with an innovative donation program coming in time for the holidays. But this colourful, rugged computer could have come from Apple, and in another time, it did.

The One Laptop Per Child organization recently announced a

donation program for the holiday season: you buy two of the XO Laptops for \$400 and you get to keep one. The other is donated to a child somewhere in the world who needs it. The program will start 11th November 2007 and you can request a e-mail notification from the site <http://laptop.org/en/index.shtml>. As far as I understand, this is the first time the machines will be sold to the public in the States. I'm looking forward to getting one.

I got some hands on time with one of the machines last January at the Macworld Expo in San Francisco. Mario Murphy, the books processing engineer at the Internet Archive (and a former member of the Berkeley Macintosh Users Group) had one for show and tell.

I was impressed with the small, green machine. The hardware's look and feel is a lot of fun and it provides an understandable software interface as well as a useful productivity package. It all looked very useable.

While it's lightweight, the hardware appeared to be rugged, with a built-in handle that I appreciated. And the keyboard was covered with a rubbery plastic that must be waterproof (we didn't test this on the show floor).

I pinged Mario the other day and he said he has seen several of them floating around the office.



“They are neat. However, the only downside for me is its keyboard. Both [in] the size and spacing of the keys and the squishy feel. In particular, I find it hard to hit a spot on the space “bar” that will produce a space character,” he told me.

“But I like that they run Debian [Linux] and that they're full computers,” he continued.

What I will appreciate in the XO is having a computer that I can take outside that won't make me worry if dust or sand blows on it, or even buries it. Or worry if I drop some water (or beer) on the keyboard. And I will be glad to have a machine that provides a full computing experience for only \$200 (or \$400 depending on how you are counting) that won't kill my wallet if it falls on the floor. That's always the worry with my MacBook Pro, even with its MagSafe power connector.

Of course, it isn't a MacBook and won't offer the rich experience of my powerful desktop substitute and Apple software. Still, for a low cost it can provide the basics: access to e-mail, a browser and productivity tools.

The XO Laptop spec sheet is available at <http://laptop.org/en/laptop/hardware/specs.shtml>

Contributed by: Ziff Davis Network

Articles

++ 'Pay By Touch' Bank Cards Launched In London.

Wireless-enabled bank cards tested in London will pave the way for a new system of cashless payments, enabling

small purchases to be made in pharmacies, newsagents, and snack bars without providing a PIN number or a signature.

The system is to be tested by around 1,000 retailers located in and around rail and bus stations across the capital. For items costing up to 10 pounds, users will pay by simply touching a reader device located at the cash till with new credit and debit cards issued by Barclaycard, Visa, or Mastercard. The cards use a short-range wireless technology known as Near Field Communication to exchange data with the reader device, which emits an audible "beep" when the transaction is completed.

By the end of 2007 it is hoped that 2,000 outlets will be involved in the scheme, Barclaycard told E-Access Bulletin. "At this stage it's a 'chicken and egg' situation. We need interest from consumers before retailers will take an interest. That's the reason we're concentrating on London to start with. In the long term - and it's difficult to say how long this will take - we expect most retailers will move over to the new system," said the spokesperson.

In future, this way of making purchases will also be available from vending machines located in places such as pubs or in the street, and also from devices such as parking meters, said Barclaycard. "The big retailers such as high street supermarkets will almost certainly take a longer time, because their existing till systems are a significant investment which has to be recouped before they think about new technology," said Barclaycard.

Fear of fraud shouldn't deter people from using the new cards, said Barclaycard. "Most card fraud is organised and involves larger sums.

But if a bank notices a pattern of unusual transactions it can request a PIN number or signature before a transaction is processed,"

Source: E-Access Bulletin

++ Braille Translations

Braille Translations provides a fast, cost-effective, high quality service of translating any document into Braille. We are able to provide Braille menus, public leaflets and business cards in Braille and help make you compliant with the Equal Opportunities Act.

We can also help with premises accessibility including Braille Tactile Signs for toilets and other doors.

++ Free EASI resources

The Barriers Are Coming Down
The fields of science, technology, engineering and math (STEM) have provided some of the toughest accessibility barriers to students and professionals with disabilities. Today's advances in information technology are providing tools and strategies to reduce these barriers and open new career paths for people with disabilities.

EASI (Equal Access to Software and Information) is sharing resources for everyone to learn more about these important transformations. All three opportunities are open to the public at no cost.

First, there is a 20-minute MP3 interview with 2 noted scientist/researchers, Dave Schleppenbach and John Gardner, who are making a difference. This is a recording of one of EASI's podcasts and will take about a minute to actually start to play using Windows Media

Player:
<http://easi.cc/download/stem1.mp3>

Second, EASI has a pamphlet which you can download and which, if you want, you can copy and share with others:<http://easi.cc/download/easistem1.doc>

Last EASI is offering a Webinar scheduled for Tuesday October 16 at 2 PM Eastern which will describe the work of the Midwest Alliance for STEM which is an NSF grant based at the University of Wisconsin but also including other regional institutions. The Webinar will let you listen to the presenters, watch as they push Web pages supporting the presentation. There will also be time for you to ask questions or make comments either using voice chat or text chat. You need to register in advance for this event. You can read more and register at: <http://easi.cc/clinic.htm>

Contributed by: Prof N. Coombs

++ YouTube SPAM

Spammers are exploiting YouTube's "invite your friends" function to send spam containing a variant of the "Storm worm."

Bradley Anstis, director of product management at [security firm Marshal](#), said that spammers are taking advantage of the YouTube function that lets people invite friends to view videos that they have viewed or posted. The function allows someone to e-mail any address from an account.

The scam on Google's video-sharing site is targeting Xbox owners, urging recipients to collect a prize version of the popular game *Halo 3*. Anstis said clicking on the link to "winhalo3"

leads to a file containing a Storm trojan.

To date, Marshal has tracked around 150,000 of the spam e-mail messages thought to have originated from YouTube accounts.

The e-mail messages are exploiting a vulnerability in the sign-up process, according to Marshal, which reported in August a Trojan designed to generate large numbers of Hotmail and Gmail accounts. A similar vulnerability is being exploited in the case of YouTube, said Anstis, adding that spammers have used intelligent character recognition (ICR) software to circumvent the verification system commonly known as Captcha. The Captcha system, in which a person must read and re-enter a selection of blurred or unevenly spaced letters and numbers into a box before being issued a new account--is used to make it harder for software programs, rather than genuine users, to sign up for services.

++ Excel 2007 calculation bug

Microsoft has made available for download patches to an Excel 2007 bug discovered late last month and is working on pushing the fix out over Microsoft Update.

<https://mail.gov.mt/exchweb/bin/redir.asp?URL=http://blogs.msdn.com/excel/archive/2007/10/09/calculation-issue-update-fix-available.aspx>

The Excel team acknowledged the obscure bug on September 24 which affected Excel 2007 and Excel Services 2007 users attempting to perform calculations of numbers around 65,535 and 65,536. Officials said Excel was calculating the values correctly, but the function in it that

takes the value and formats it to be displayed on the screen was faulty

Question Box

This month, as promised to the many readers who wrote to us on this subject, we are including step-by-step tips on how to use the Internet safely and safeguarding your privacy.

++ Help keep spam out of your inbox

Block images

Just as a lighthouse beacon beams a message with light, pictures in e-mail messages--also called "Web beacons"--can be adapted to secretly send a message back to the sender.

Spammers rely on information returned by these images to locate active e-mail addresses. Images can also contain harmful code and be used to deliver a spammer's message in spite of filters.

The best defence against Web beacons is to prevent pictures from downloading until you've had a chance to review the message.

Both MSN Hotmail and Microsoft Outlook 2003 are preset to do this automatically for e-mail from addresses not in your address book. Outlook Express also increases its protection against Web beacons if you're using Windows XP Service Pack 2.

Keep your filters current

Spam is a cat-and-mouse game with spammers working relentlessly to outwit the filters. Do your part by keeping your junk e-mail filter up to date. To do this if you're using Outlook

2003, go to Microsoft Update at <http://update.microsoft.com/microsoftupdate>, and follow the instructions on the screen.

Be careful about sharing your e-mail or instant message address

- Only share your primary e-mail address with people you know. Avoid listing your e-mail address in large Internet directories and job-posting Web sites. Don't even post it on your own Web site (unless you disguise it as described below).
- Set up an e-mail address dedicated solely to Web transactions. Consider using a free e-mail service to help keep your primary e-mail address private. When you get too much spam there, simply drop it for a new one.
- Create an e-mail name that's tough to crack. Try a combination of letters, numbers, and other characters--Don2Funk9@example.com or J0e_Y0ng@example.com (substituting zero for the letter "O"). Research shows that people with such names get less junk e-mail.
- Disguise your e-mail address when you post it to a newsgroup, chat room, bulletin board, or other public Web page--for example, SairajUdin AT example DOT com. This way, a person can interpret your address, but the automated programs that spammers use often cannot.



- Watch out for pre-checked boxes. When you buy things online, companies sometimes pre-select check boxes by which you indicate that it's fine to sell or give your e-mail address to responsible parties. Clear the check box if you don't want to be contacted.
- When you sign up for Web-based services such as banking, shopping, or a newsletter, carefully read the privacy policy before revealing your e-mail address so you don't unwittingly agree to share confidential information. The privacy policy should outline the terms and circumstances regarding if or how the site will share your information. If a Web site does not post a privacy statement, consider taking your business elsewhere.

Improve your computer's security

You can greatly reduce your risk from hackers, viruses, and worms if you use a firewall, keep your Windows and Office software up to date, and install antivirus software (and update it routinely).

What to do about spam you already received?

- Delete junk e-mail messages without opening them. Sometimes even opening spam can alert spammers or put an unprotected computer at risk.
- Don't reply to spam unless you're certain that the message comes from a legitimate source. This includes not responding to such messages that offer an option to "Remove me from

your list." Do not "unsubscribe" unless the mail is from a known or trusted sender.

- Update your e-mail junk mail program and e-mail filters. Spammers continually try new tricks, trying to bypass anti-spam technologies. The Outlook Junk E-Mail Filter is powered by Microsoft SmartScreen technology, which helps prevent spam from cluttering your inbox. Updates are available from the Office Update and Microsoft Update and can be downloaded automatically, providing you up-to-date protection against spam and phishing.
- Don't give personal information in an e-mail or instant message. It could be a trick. Most legitimate companies won't ask for personal information by e-mail.
- If a company you trust, such as your credit card company or bank, appears to ask for personal information call the company using a number you retrieve yourself from the back of your credit card, a bill, phone book, or the like- NOT a number from the e-mail message. If it's a legitimate request, the company's customer service department should be able to help you.
- Think twice before opening attachments or clicking links in e-mail or instant messages, even if you know the sender. If you cannot confirm with the sender that an attachment or link is safe, delete the message.

- If you must open an attachment that you're less than sure about, save it to your hard disk first so that your antivirus software can check it before you open it.
- Don't buy anything or give to any charity promoted through spam. Spammers often swap or sell the e-mail addresses of those who have bought from them, so buying something through spam may result in even more spam.
- Plus, spammers can make their living (and a lucrative one, too) on people's purchases of their offerings. Resist the temptation to buy products through spam, and help to put spammers out of business.
- Criminals use spam to prey on people's desire to help others. If you receive an e-mail request from a charity you'd like to support, avoid donation scams by calling the organization directly to find out how to contribute.
- Don't forward chain e-mail messages. Not only do you lose control over who sees your e-mail address, but you also may be furthering a hoax or aiding in the delivery of a virus.
- Plus, there are reports that spammers start chain letters expressly to gather e-mail addresses. If you don't know whether a message is a hoax or not, a site like Hoaxbusters can help you separate fact from fiction.
- It can be troubling to receive spam from what appears to be your own account. Your first suspicion may be that someone has hacked into your account to send you mail-or worse, send others e-mail that is allegedly from you. The truth is these fears are not likely to be real. More likely, a spammer has forged the headers (which include your e-mail address) to lend authenticity to their junk e-mail, and also potentially help the message bypass some e-mail filters.

Report fraudulent, abusive e-mail

If you receive abusive, harassing, or threatening e-mail messages or have been the target of a phishing e-mail scam, report it. If nothing else, perhaps you'll save someone else from becoming a victim.

- Report abusive, harassing, or threatening e-mail messages to your Internet Service Provider (ISP).
- Report phishing scams and other fraudulent e-mail to the company that has been misrepresented. Contact the organization directly and not through the e-mail you received.
- If you use web mail these often provide a JUNK or SPAM reporting button, with which you can report junk e-mail before you even open it.
- File a complaint with the U.S. Federal Trade Commission (FTC). First review the FTC tips for fighting spam

<http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm>), and then file your complaint at https://rn.ftc.gov/pls/dod/wsolic_startup?Z_ORG_CODE=PU01

Forward your complaints to system administrators who can act on them with the assistance of the Network Abuse Clearinghouse at <http://www.abuse.net/>.

++ Pump-and-dump scams

Who couldn't use a tip on a hot stock? Be warned: When the tip comes unsolicited in your e-mail inbox, it's probably a scam.

The 'pump-and-dump' scam is a common form of spam these days. According to the United States Security and Exchange Commission (SEC), spammers send 100 million of these e-mail messages per week!

How pump-and-dump scams work

Scammers buy stock in a small company, often with stock prices of only a few dollars per share. Then they send out millions of e-mail or text messages across the globe to encourage recipients to buy that stock. These messages can even be disguised as confidential information that was sent to the recipient by mistake.

When enough people buy the stock, the price of the stock goes up. When the price is high enough, the spammers sell their shares. The price goes back down, and people who purchased the stock as a result of the tip suffer.

It can be difficult to find out who's behind pump-and-dump e-mail scams. That's because spammers can take control of large numbers of computers and turn them into zombies that can work together as powerful 'botnets' to send the spam messages out.

What you can do to avoid pump-and-dump scams

- Use spam filtering technology. For more information, see the article - *Help keep spam out of your inbox above*.
- Don't make investment decisions based on anonymous e-mail or text messages you receive.
- Don't open attachments in unsolicited e-mails. To avoid being caught by spam filters, stock spam usually is sent as an image or as a PDF attachment.

++ 11 tips for safer instant messaging

1. Be careful when creating a screen name. Each IM program asks you to create a screen name, which is similar to an e-mail address. Your screen name should not provide or allude to personal information. For example, use a nickname such as SoccerFan instead of BaltimoreJenny.
2. Create a barrier against unwanted instant messaging. Do not list your screen name or e-mail address in public areas (such as large Internet directories or online community profiles) or give them to strangers.
3. Some IM services link your screen name to your e-mail address when you register. The easy availability of your e-mail address can result in your receiving an increased number of spam and phishing attacks.

4. Never provide sensitive personal information, such as your credit card numbers or passwords, in an IM conversation.
5. Only communicate with people who are on your contact or buddy lists.
6. If you decide to meet a stranger that you know only from IM communication, take appropriate safety precautions. For example, do not meet that person alone, (take a friend or parent with you), and always meet and stay in a public place, such as a cafe.
7. Never open pictures, download files, or click links in messages from people you don't know. If they come from someone you do know, confirm with the sender that the message (and its attachments) is trustworthy. If it's not, close the instant message.
8. Don't send personal or private instant messages at work. Your employer might have a right to view those messages and they have little to do with work anyway.
9. If you use a public computer, do not select the feature that allows you to log on automatically. People who use that computer after you may be able to see and use your screen name to log on.
10. Monitor and limit your children's use of IM. Limiting or prohibit use of technology is a very short term solution. It is best to educate the users on the

potential pitfalls, as this addresses their life long needs.

11. When you're not available to receive messages, be careful how you display this information to other users. For example, you might not want everyone on your contact list to know that you're "Out to Lunch."

++ How to use social networking Web sites more safely

You may already know that blogging—keeping a public "Web log" or personal journal online—is common among teens and even younger kids.

Now you can also create personal Web pages on social networking Web sites hosted by services like Windows Live Spaces, MySpace, Friendster, Facebook, and others. These Web pages can often be viewed by anyone with access to the Internet.

With these services, which are extremely popular among teenagers, kids can fill out profiles that can include:

- Photos
- Videos
- Personal information such as full names, locations, and cell phone numbers

Often the services that host the social networking sites provide several different ways for people to communicate with one another, including blogging and instant messaging features.

You can use social networking sites to connect with people who might live

halfway around the world and with people whom you meet every day.

Social networking can provide a helpful way for kids to express their emotions or even to perform unofficial background checks on other kids they meet at parties and at school. For example, after they meet another kid in person, a kid might visit that other kid's Web site to find out if he or she might be someone they'd like to be friends with.

Unfortunately, the information that kids post on their pages can also make them vulnerable to predators.

Here are some ways you can help your kids can use social networking Web sites more safely.

- Set your own house Internet rules. As soon as your children begin to use the Internet on their own, it is a good idea to come up with a list of rules that you can all agree on. These rules should include whether your children can use social networking Web sites and how they can use them.
- Ensure your kids follow age limits on the site. The recommended age for signing up for social networking sites is usually 13 and over. If your children are under the recommended age for these sites, do not let them use the sites. It is important to remember that you cannot rely on the services themselves to keep your underage child from signing up.
- Educate yourself about the site. Evaluate the site that your child plans to use and read the privacy policy and code of conduct carefully. Also, find out if the site monitors content that people post on their pages. Also, review your child's page periodically.
- Insist that your children never meet anyone in person that they've communicated with only online, and encourage them to communicate only with people they've actually met in person. Kids are in real danger when they meet strangers in person whom they've communicated with only online. You can help protect your children from that danger by encouraging them to use these sites to communicate with their friends, but not with people they've never met in person.
- It might not be enough to simply tell your child not to talk to strangers, because your child might not consider someone they've "met" online to be a stranger.
- Ensure your kids don't use full names. Have your children use only their first names or a nickname, but not a nickname that would attract the wrong kind of attention. Also, do not allow your children to post the full names of their friends.
- Be wary of other identifiable information in your child's profile. Many social networking sites allow kids to join public groups that include everyone who goes to a certain school.

- Be careful when your children reveal this and other information that could be used to identify them, such as where they work or the name of the town they live in, especially if it is a small one.
- Consider using a site that is not very public. Some social networking sites allow you to password-protect your site or use other methods to help limit viewers to only people your child knows. With MSN Spaces, for example, you can set permissions for who can view your site, ranging from anyone on the Internet to only people you choose.
- Be smart about details in photographs. Explain to your children that photographs can reveal a lot of personal information. Encourage your children not to post photographs of themselves or their friends with clearly identifiable details such as street signs, license plates on their cars, or the name of their school on their sweatshirts.
- Warn your child about expressing emotions to strangers. You've probably already encouraged your kids not to communicate with strangers directly online. However, kids use social networking Web sites to write journals and poems that often express strong emotions.
- Explain to your children that these words can be read by anyone with access to the Internet and that predators often search out emotionally vulnerable kids.
- Communicate with your children about their experiences. Encourage your children to tell you if something they encounter on one of these sites makes them feel uncomfortable or threatened. Stay calm and remind your kids they are not in trouble for bringing something to your attention.
- Remove your child's page. If your children refuse to abide by the rules you've set to help protect their safety, you can contact the social Web site your child uses and ask them to remove the page. You may also want to investigate Internet-filtering tools (such as MSN Premium's Parental Controls) as a complement to—not a replacement for—parental supervision.

++ How to tell fact from opinion on the Internet

The Internet offers tremendous resources and learning opportunities, but it also contains a great deal of information that may be neither helpful nor reliable.

Because anyone can post comments or information on the Internet, users need to develop critical-thinking skills to judge the accuracy of online information.

This is particularly true for new users who tend to believe that, "If it's on the Internet, it must be true."

Traditionally, printed resources have had gatekeepers—such as editors,

proofreaders, and fact checkers—to weed out mistakes, lies, and inaccurate information. The Internet, however, in many cases has no safety guards when it comes to checking the validity of information posted online.

- Even preschool students are now using the Internet to look up information, so it's important to teach them early to distinguish fact from opinion and how to recognize bias, propaganda, and stereotyping.
- Think about information you find online. For example, what is the purpose of the site? To entertain? To sell? Does the site contain contact information for the author or an "About Us" section?
- Is the site sponsored by a certain company, a person, or is it a public conversation? Is the Internet the best place to find the information you're searching for?
- Make sure you check the online information they collect against other sources. Refer to other Web sites or media—such as newspapers, magazines, and books—to verify the information.
- Use a variety of information resources, not just the Internet. It may feel retro, but visits to the library can be a very educational experience. Also, consider buying a good encyclopaedia on CD-ROM. This will give you access to alternative sources of information.

- Read the help pages of search engines, to learn the techniques to effectively search out information online. This will greatly improve your ability to obtain quality information.
- Discuss hatred and racism with your kids. Software filters can help block some of this type of material. Your kids, however, should learn about racism and world events so they can recognize hateful content.

++ RATs: Remote Access Trojans and how to help avoid them

Remote Access Trojans (RATs) are malicious software programs that criminals can use to control your computer through your Internet connection. A RAT can let a criminal view and change your computer's files and functions, monitor and record your activities, and use your computer to attack other computers without your knowledge.

How RATs get on your computer

RATs often come hidden in illicit software and other files and programs that you might download from the Internet. They can also appear in e-mail or instant messages disguised as attachments or links to funny images, greeting cards, or audio and video files.

If you click the attachments or links to open them, a RAT might be secretly downloaded. Sometimes a RAT can even get on your computer without any action from you, by taking advantage of vulnerabilities in software or the Internet.

Some RATs are used to form zombie armies, which are large groups of computers that criminals control to perform tasks such as overwhelming servers with messages, or spreading viruses or spyware.

How to help keep RATs away

- Practice safe online communication. Only share your primary e-mail address with people you know. Avoid listing your e-mail address in large Internet directories.
- Don't open attachments in e-mail or instant messages unless you're sure what they are and who they're from.
- Check carefully before you run, download, or use any software that doesn't come from well-known, trustworthy sources.

- Use a firewall. A firewall is a software program or piece of hardware that can help screen out RATS or other malicious software. If you use Windows Vista or Windows XP Service Pack 2 (SP2) you have a firewall built-in and turned on by default.
- Keep your computer up to date. Visit Microsoft Update at www.windowsupdate.com to help make sure you've got the latest updates for your computer.
- Use antivirus software and keep it up to date. Antivirus software can help protect against some RATs.

Use antispyware software and keep it up to date. Antispyware software, such as Windows Defender can offer protection from some RATS. Windows Defender comes with Windows Vista. If you use Windows XP SP2, you can download Windows Defender for no charge.

Credits

FITA's services are made possible thanks to the support of the following funding partners.

- Malta Information Technology and Training Services Ltd.
- National Commission Persons with Disability
- Gasan Group of Companies
- Computime Ltd.
- Philip Toledo Ltd
- Megabyte Ltd
- The Computer Society of Malta
- SMS Group of Companies
- Crimsonwing (Malta)
- 6PM Consultancy Group
- Engineering Centre

Disclaimer

The reader is responsible for the use of information contained herein and its safe and lawful use. This includes work policies and restrictions applicable to the computer environment specific to the user. Descriptions of products or services are for information purposes only.

FITA makes no claim, representation or warranty, express or implied, as to the information presented here, the performance of products and services, or any results that may be obtainable by their use. FITA also does not necessarily endorse the specific content or positions contained in the articles shown or referred to.