

Microsoft Office Productivity

Three ways to protect your Excel data with confidence

Information Systems Protection

Twelve ways to harden your domain controllers and prevent security breaches

Web Design & Development

Employ interactive elements to keep users on your site

From the Editor

Sometimes you need to keep your Excel data away from prying eyes. But you can protect your data in so many ways that the whole process gets confusing. We'll break it down for you so your data never stays vulnerable.

Domain controllers (DCs) hold a lot of valuable information about your Windows server, which means that you must secure them. We've compiled a few ways for you to keep intruders out of your network by strengthening your domain controllers.

Finally, nothing drives away online visitors like a boring website. We'll introduce you to a few ideas for adding interactive elements to your site so visitors want to stay.

MICROSOFT OFFICE PRODUCTIVITY

Three ways to protect your Excel data with confidence

If you share workbooks, you probably grumble over the changes your colleagues make to your workbooks' layout. Or maybe someone inadvertently deleted a formula that you worked hard to build. To preserve your workbooks and their individual worksheets, you need to understand the different levels of protection Excel offers. We'll familiarize you with Excel's three defensive measures: workbook protection, worksheet protection and range-level protection.

1. Lock down the entire workbook

Workbook protection affords you sweeping security because it protects the entire workbook. You can even add a password if you want only certain people (or just yourself!) to access the workbook data.

To protect your entire workbook with a password:

1. Launch Excel and open the workbook you'd like to protect.
2. Choose Tools | Protection | Protect Workbook from the menu bar to open the Protect Workbook dialog box.
3. Select the Windows check box if you want to preserve your window

arrangement. The Structure check box is selected by default.

4. Enter a password in the Password (Optional) text box if you'd like to assign one to your workbook, as shown in **Figure A**.
5. Click OK. If you entered a password, re-enter the password in the Confirm Password window that displays and click OK again.

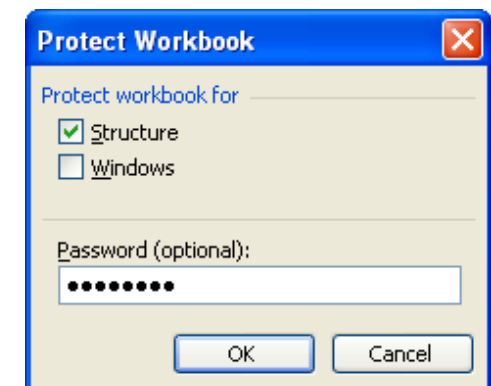
Just remember that you cannot retrieve your password if you forget it later. Make sure you choose a memorable password so that you don't lose access to your workbook.

When you've protected your workbook for structure, you'll notice that users can't insert, delete, rename, move or copy

Related Courses

- Excel 2003 - Levels 1, 2, and 3
- Excel 2007 - Levels 1, 2, and 3

worksheets within the workbook. You also can't change a worksheet tab's color. If you protect the workbook for windows, you can't rearrange worksheets, add or remove a window split, or freeze/unfreeze



A Without a password, any savvy Excel user can turn off your protection and make changes

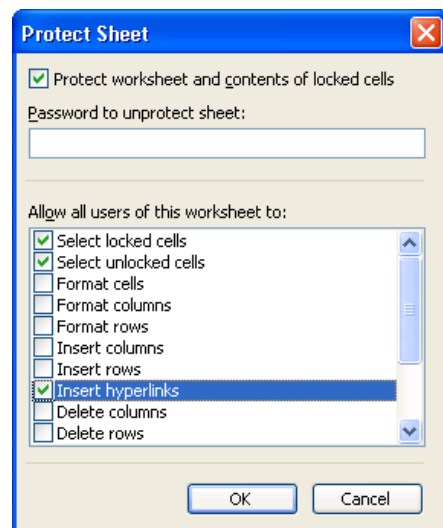
windows. But you can still hide or unhide worksheets.

To turn off workbook protection:

1. Choose Tools | Protection | Unprotect Workbook from the menu bar to display the Unprotect Workbook dialog box.
2. Enter your password (passwords are case-sensitive) in the text box provided.
3. Click OK to disable the workbook's protection.

2. Prevent unwanted worksheet changes

There are two steps to protecting a worksheet in your workbook:



B We'll allow users to insert hyperlinks in our worksheet, even though it's still protected.

1. Lock the items you want to protect.
 2. Protect your worksheet.
- The locking concept trips up most Excel users, so let's take a look at that step first.

Unlock cells you don't need to protect

The tricky part to locking your worksheet data is that Excel locks your cells by default. But locked cells differ from protected cells. Excel won't protect your worksheet until you enable protection (even though your cells are locked by default). You actually need to *unlock* the cells that you want to permit users to modify before you protect the worksheet.

To unlock a cell or range of cells:

1. Select the cell or data range you want to unlock. (If the cells are noncontiguous, hold down the [Ctrl] key as you select them.)
2. Choose Format | Cells from the menu bar.
3. Select the Protection tab.
4. Deselect the Locked check box.
5. Click OK to allow users to change your selected cells or data range.

Take note: If the Locked check box is grayed out, some of the cells you selected are already unlocked. To ensure that all of your selected cells are unlocked, keep clicking in the Locked check box until it's empty.

Protect more than just cells

Keep in mind that you can also unlock objects, like charts or AutoShapes. Follow the same procedure as you did with unlocking cells, but choose the Format menu that applies to your object (e.g., Format | Chart to unlock a chart).

Enable worksheet protection

Once you've unlocked the cells you want users to have access to (which means that the rest of the worksheet remains locked by default), it's time to enable worksheet protection.

To protect your sheet's locked cells:

1. Choose Tools | Protection | Protect Sheet from the menu bar.
 2. In the Protect Sheet dialog box, select the check box(es) for functions that you want to allow in spite of your worksheet protection in the Allow Users Of This Worksheet To panel, as shown in **Figure B**. By default, Excel allows users to select both locked and unlocked cells when the worksheet is protected.
 3. Enter a password in the Password To Unprotect Sheet text box if you'd like.
 4. Click OK when you're ready to enable worksheet protection.
- If you want to disable this worksheet protection, just choose Tools | Protection

| Unprotect Sheet from the menu bar. Enter your password if you assigned one to the worksheet protection.

3. Create range-specific protection

In Excel 2002 and later, you can further customize your worksheet protection by password-protecting only specific data ranges — and by giving only certain network users or groups access to data.

Pinpoint your protection

Instead of protecting an entire workbook — or even an entire worksheet — you can assign different passwords to separate data ranges. For instance, you could protect ranges that only the accounting staff should change while also assigning a different password to a range in the same worksheet to protect human resources data.

To assign a password to a specific data range:

1. Make sure your worksheet is unprotected (if not, choose Tools | Protection | Unprotect Sheet from the menu bar.)
2. Select the data range you want to assign a password to.
3. Choose Tools | Protection | Allow Users To Edit Ranges from the menu bar.
4. Click the New button in the Allow

Users To Edit Ranges dialog box. The New Range dialog box appears and the range you've already selected is filled in.

5. Rename the range in the Title text box. We named ours *HR Only*.
6. Enter your case-sensitive password in the Range Password text box.
7. Click OK. Re-enter your password in the confirmation box and click OK to return to the Allow Users To Edit Ranges dialog box.

You'll see your new range listed in the Allow Users To Edit Ranges dialog box,

Adapt for Excel 2007

Workbook, worksheet and range protections work similarly in Excel 2007. You can find the options you need to set up data protection on the Review ribbon in the Changes area.

as shown in **Figure C**. You can add more ranges by repeating these steps.

To protect your listed ranges:

1. In the Allow Users To Edit Ranges dialog box, click the Protect Sheet button.
2. Change any protections you'd like, just as you would when you're protecting an entire worksheet, in the Protect Sheet dialog box.
3. Click OK to activate your worksheet protection.

Now, whenever someone tries to change the data within a protected range, they must provide the password you specified.

Allow only certain people to access a data range

To eliminate some of the hassle that comes with so many passwords — some given

to entire departments — you can let your network authenticate users for you.

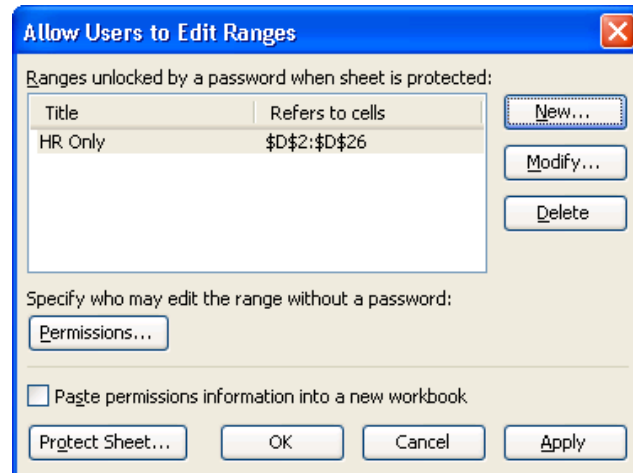
To permit only certain network users or groups access to a range:

1. Unprotect your worksheet.
2. Choose Tools | Protection | Allow Users To Edit Ranges from the menu bar to open the Allow Users To Edit Ranges dialog box again.
3. Choose a range from the list box and click the Permissions button to display the Permissions For Range dialog box.
4. Click the Add button to display the Select Users, Computers, Or Groups dialog box.
5. Enter a network username in the list box and click the Check Names button to verify the name. If Excel recognizes the network group or user, Excel underlines the username.

6. Click OK when you're ready. The users and groups that you've granted permission to that data range display in the Permissions For Range dialog box.
7. Click OK until you've dismissed all open dialog boxes and accepted the range permissions.

Version difference: Excel 2002 and 2003 have slightly different permissions dialog boxes. Excel 2003 added the ability to grant permission to a specific computer based on its computer name in addition to network users and groups.

Once you give an individual, group or computer permission to edit a data range, the user can do so without a password. However, you should still assign a password to the range. Otherwise, any user will be able to edit the range even if you haven't given that user permission. 🌐



C
Create, edit or delete your protected ranges from the Allow Users To Edit Ranges dialog box.

Business skills for the new world of work

In business today, productivity is key to your success. Whether that means setting up projects for success, forecasting and analyzing trends, or managing critical business information, it is vital that you have the skills to work at peak performance. You already know how to use Microsoft® Office System applications. New Horizons offers Microsoft Business Skills Series Courses to teach you how to use those applications to more efficiently manage, work with, and prioritize information to make better decisions. Go to www.NewHorizons.com for information on courses that cover topics such as:

- 🕒 4001 Team Collaboration Using Microsoft SharePoint Services
- 🕒 4003 Summarizing Microsoft Office Excel 2003 Data to Make Better Business Decisions
- 🕒 4006 Time and Task Management Using Microsoft Office Outlook 2003

Twelve ways to harden your domain controllers and prevent security breaches

Domain controllers are the servers that control the security and administration of a Windows domain. The domain controllers are, in many ways, the most critical servers on your network, because they store the Active Directory (which holds information about all objects — computers, users, and other resources — on the network) and perform authentication. The DCs are also the repository for Group Policy information that's applied to computers and users on the network.

If an attacker takes over or takes down a domain controller, important security information can be compromised and the operation of the network can be disrupted. However, you can take steps to make your DCs more secure.

Deploy DCs securely

You should ensure that physical access to domain controllers is limited right from the beginning. If a DC will be located in a remote location, install and configure it in a controlled, secure environment and then transport it to the destination using a secure method.

Ensure that DCs are kept in a physically secure room with strong access controls, such as key card entry, logging of time in and out, video monitoring, etc.

Make the machines physically secure by removing floppy disk drives, CD/DVD writers, USB ports, and other

means by which data could be uploaded to or downloaded from the machine.

Place domain controllers

You should place domain controllers on secured network segments. Each DC should be on the same network segment as its clients.

If you place a domain controller on a perimeter network, you should put it behind a standalone router to ensure that internet users can't directly access it.

Disable non-essential services

Best security practice is for domain controllers to be dedicated to that task. That is, a domain controller should not also be a web server, a remote access/VPN server, etc. That's because additional services running on the domain controller provide vulnerabilities that could be exploited by attackers.

You should disable all non-essential services on all servers, but especially on domain controllers.

Note: Windows Server 2003 doesn't install Internet Information Services (IIS) by default, but Windows 2000 Server does.

Some other services that you should usually disable on dedicated domain controllers include:

- Fax service
- Indexing service
- Internet connection sharing (ICS)
- Removable storage
- Routing and Remote Access (RRAS)
- Telephony
- Telnet (unless used for remote administration)

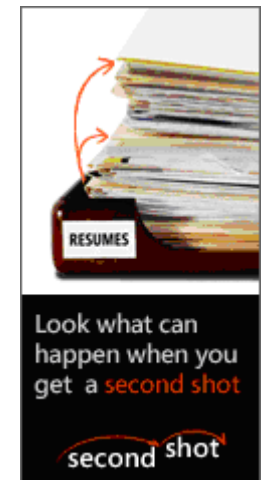
- Terminal services (unless used for remote administration)

Secure Active Directory

The first step in securing Active Directory is to establish security and administrative boundaries: AD forests, domain trees, and domains.

Related Courses

- 2279 Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure
- 2823 Implementing and Administering Security in a Microsoft Windows Server 2003 Network



Plan how to delegate administrative authority within each security boundary. Consider when and how to use isolation to prevent administrators from overstepping their boundaries. To isolate the users, computers, and administrators in a particular department, division, or other business unit, you must deploy multiple forests, which may require that you establish external trusts so users can collaborate across forests.

Secure AD files

When you promote a server to DC, by default, the Active Directory database, SYSVOL folder, and log files are stored on the system volume. You can — and should — specify a different location for these files during the promo process. Hackers expect the files to be in the

default location and hacker tools will look for them there.

Putting the AD database and SYSVOL on a different physical disk from the system volume prevents them from being affected by some types of attacks that are aimed at the system volume.

If the server is already a domain controller, you can move the database and SYSVOL folder to a different drive.

Note: You can move SYSVOL with the Active Directory Wizard by installing Active Directory and reinstalling it after SYSVOL is moved. A better alternative is to move the SYSVOL folders manually.

Disable permissions compatibility

For backward compatibility, Windows 2000 Server and Server 2003 domain controllers can be configured so that Windows NT server services, such as NT Routing and Remote Access Service (RRAS), will work properly.

Allowing permissions compatible with NT servers creates a security issue because the Everyone group (which includes anonymous users) will be given Read permissions on all user, computer, and group objects in the directory.

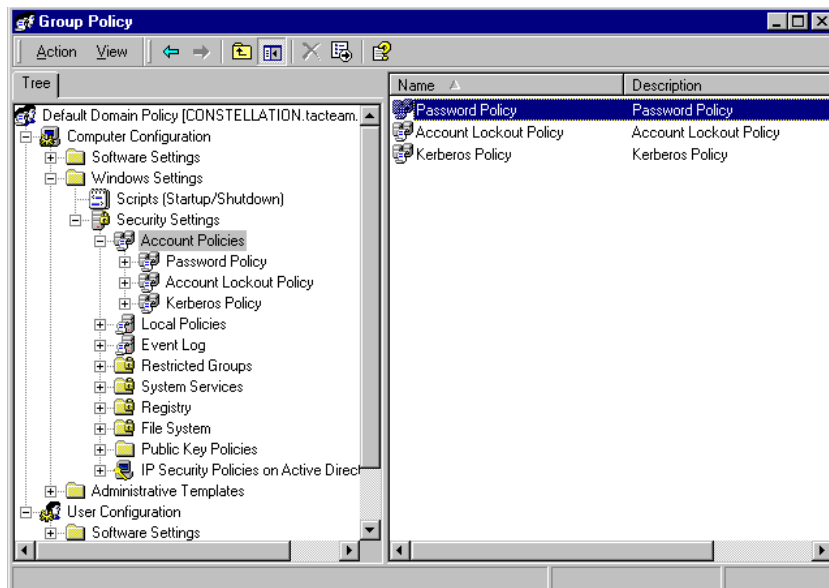
Don't enable permissions compatibility unless you must do so because you have legacy applications that need to use anonymous access to query the directory.

Apply service packs and patches

Another important element in securing Active Directory is to ensure that the proper service packs are applied or the proper operating system(s) used so that LDAP (Lightweight Directory Access Protocol) data that's sent to Active Directory will be signed. To do so, ensure that the proper service packs are applied to both the domain controller servers and the client machines that communicate with them, as follows:

A

Set and enforce password policies through Group Policy.



- Windows XP clients should have Service Pack 1 or above applied.
- Windows 2000 servers should have Service Pack 3 or above applied.
- Windows Server 2003 supports signed LDAP traffic out of the box.

All machines should have the current security fixes applied. The patches can be distributed via Windows Update/Microsoft Update, Windows Software Update Services (WSUS), or Systems Management Server (SMS).

Integrate AD with your firewall/VPN server

You can use Internet Security and Acceleration (ISA) Server 2004 for your firewall and VPN server. This allows you to integrate firewall and VPN users with your Active Directory domain accounts.

You can also integrate Active Directory with Check Point's VPN server and firewall.

Protect domain account passwords

You should establish and enforce password policies through Group Policy. For example:

- Enforce password history: Set to at least 24.
- Maximum password age: Set to 30-45 days.
- Minimum password length: Set to at least 8 characters.

- Password complexity requirements: Enable.

The password policy is set through the Default Domain Policy, in the Computer Configuration | Windows Settings | Security Settings | Account Policies node, as shown in **Figure A**.

Administrator accounts merit special protective measures. Implement multi-factor authentication (smart card, token, or biometrics) for admin logons.

Use Syskey

Domain controllers store the passwords for domain accounts in the Active Directory database. You can encrypt the password information with the Syskey utility, and you can further secure your domain controller by requiring a password to start up the computer.

For best security, store the key on a floppy disk instead of storing it on the hard disk. An intruder who gains physical access to your domain controller won't be able to start the machine without inserting the floppy disk.

To run the Syskey tool:

1. Select Start | Run and type *cmd* to open a Command Prompt window.
2. At the prompt, type *syskey*.
3. The Encryption Enabled option should be selected.
4. Select Password Startup, and then type in a strong password.

5. Select System Generated Password, and then select Store Startup Key On Floppy Disk if you want the best security.

Use Group Policy security templates

You can use security templates and Windows group policy to configure your domain controllers more securely. Windows Server 2003 contains a number of built-in security templates, including:

- Securedc.inf, which increases domain controllers' security.
- Hisecdc.inf, which increases security of domain controllers to an even greater degree.

Apply security templates

You apply the security templates using the Security Analysis and Configuration console.

To open the console:

1. Select Start | Run.
2. Type *mmc* to create a new console.
3. Open the File menu (or the Console menu in Windows 2000) and select Add/Remove Snap-in.
4. Select Security Configuration and Analysis from the list of snap-ins.
5. Click Close and then OK.
6. In the Security Configuration and Analysis console's left pane, right-

click on the top-level node and select Open Database.

7. Type the name of the database file in the File Name box and click Open.
 8. Select the template you want to apply and click Open to import the template entries.
 9. Right-click on the top node in the left pane again and select Configure Computer Now.
- You can import the template you want to use into the database by clicking Action | Import Template and selecting the appropriate template.

Get additional security templates

You can find additional templates, including High Security – Domain Controller.inf, in the **Windows Server 2003 Security Guide**. The templates are contained in the Tools And

Templates folder. The guide itself provides additional information on using the templates to harden your domain controllers.

Use the Security Configuration Wizard

Windows Server 2003 Service Pack 1 includes the Security Configuration Wizard (SCW), which you can install through the Add/Remove Programs applet after installing the service pack.

You can use the Wizard to create security policies based on server role (e.g., the domain controller role).

For more information about the SCW, see www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/38f0693d-59eb-45ca-980d-31fe03eb54df.mspix.

Graphic & Design eTips to Enhance Your Work



If you are an expert at what you do, then you want to sign up for FREE New Horizons Graphics & Digital Designer eTips. Each week you will receive expert advice from our experienced editors that will improve your productivity and enhance your work. Learn more about the applications you use everyday, including: Adobe Illustrator, Adobe InDesign, Adobe Pagemaker, Adobe Photoshop, Digital Photography and QuarkXPress. Imagine the possibilities with the skills you'll gain!

Employ interactive elements to keep users on your site

Bored with the stillness of your web pages? We often tend to think of our websites as relatively static. There are a number of things you can do to make them more active, even inviting, to your viewers, and let them actually participate in your site. To really get people going, you need to make your website interactive, allowing them to become part of the website rather than casual observers.

Activate interactivity

In this article, we'll discuss the need for interactivity on the web. First we'll examine the specific requirements of interactivity from different users' perspectives. Then, we'll explain the different ways to implement interactivity to your site through CGI, Macromedia Flash, Java, and free internet web tools.

Interact with the audience

Whether a user is surfing the web as a student, a business owner, or a thrill seeker, before she starts browsing she knows the interactive elements she's looking for. By figuring out your target audience's interactive needs, you can incorporate those interactive elements into the websites you're designing.

A student's interactive needs

In the world of education, pencils and note pads are slowly being replaced with laptops and laser printers. It's

advantageous for teachers to fully examine the unlimited possibilities of the internet. If you're a teacher who provides online tutorials, interactivity is a must. Adding interactivity will engage the student and maintain interest in the class. It's efficient and potentially livelier than studying from a text book.

There are some simple interactive teaching methods to consider when designing a website for educational purposes. Providing a student with online testing or adding a chat or search area about the topic enriches the learning experience. Interactive online activities encourage students to become involved with a subject which, in turn, helps them to retain the subject matter.

A business' interactive needs

For the business professional, there are many interactive elements on a website that will engage a user. One may include a contact page with an online order form, as shown in **Figure A**, that visitors can

submit. Another may be to offer periodic online chats with guest speakers who can discuss the topics your visitors are interested in. Or, provide weekly tips, helpful hints, or links to sites that have related information. For those who want to boost their revenue providing online business transactions is a must. Incorporate secure eCommerce and bill paying options into your website designs. The customer will love you!

A fun seeker's interactive needs

Though users are relying more and more on the internet for their professional and task-driven needs, there are still those who are only after one thing when they search the web ... FUN. Some people even use the internet as their favorite broadcast entertainment medium. These people are strictly exploring entertainment, or investigating new technologies and online features.

Sometimes they have a subject in mind, such as a movie trailer they

want to view, a particular song they want to hear, or a game they want to play. Whatever the entertainment reason, fun seekers expect to have more graphics and interactive features. Users tend to be more lenient on download times than those doing business transactions. When designing for the fun seeker, be sure to provide a high "wow" factor with your games, music, or movie clips, but don't let it cloud the usability or your users will go elsewhere.

We've given you some ideas for interactivity depending on the needs of your audience. Now that you see the need for interactivity, let's discuss how you can apply these interactive elements to your website.

Choose your web tool

Web designers now have greater flexibility and graphical layout options with HTML than when it was first created. By itself, HTML provides little interactivity beyond the ability to skip between

Related Courses

- Flash CS3 Levels 1 and 2
- JavaScript - Enhancing Web Pages

sections of a document or from one page to another.

Regardless of the limitations of HTML, there are ways to turn a static site into a dynamic or interactive one, enabling visitors to do a number of useful things. For example, readers can search for information in a database, fill out a form, or play a game. We'll address four ways of accomplishing this: a common gateway interface (CGI), Flash, JavaScript, and web-based internet tools.

Common Gateway Interface (CGI)

The most common use of CGI scripts is for implementing image maps and online forms. They're valuable tools used to their full potential when they're used for email forms or data-entry boxes. The forms can function as simple Perl scripts for surveys to complex purchase order forms.

A web server must be running a CGI application designed to process

the information that visitors submit. The CGI application transfers the data that's entered into a web page form by the user into a database on the web server. The script is usually a link between the server and a database. Most of the work happens on the server, behind the scenes. You only witness the result. The beauty of CGI is that it allows this sort of two-way communication through the use of HTML.

Flash

Another widely used interactive tool is Flash. Flash is an animation and authoring program specifically developed for use on the web. You can use Flash to create an entire web page or site and incorporate text, graphics, interactive buttons, and animation. You can embed interactive Flash elements to a static HTML page. This method of web design is a good compromise between the complexity of development and

visual effect you can achieve. It also saves you development time and resources compared to a pure Flash project. Some examples of Flash interactive elements are site navigation, animated icons, movies, and sound effects.

Java

Although Flash can provide sophisticated interactive effects for the web, the real breakthrough in interactivity and multimedia content delivery is a programming language called Java. Like a gateway script, Java is activated by a special HTML tag. Unlike CGI scripts that require information on the server to run applications or process input, Java enables developers to create content that can be delivered to and run by users. It supports anything from spreadsheets and tutorials to interactive games and animation.

Java applets are complete programs written in Java language that are called by and may appear within a web

page but are not part of the page. Java can be database interfaces, games, or any number of other applications. Rather than just providing text, sound, images, or videos to observe, a Java page offers a place to play, learn, interact, and communicate with others without going elsewhere through hyperlinks.

Websites, such as www.bravenet.com, which hosts interactive elements, provide you with free easy installation code to cut and paste into your web pages. Then, you can customize the interactive elements to suit your needs. The only drawback is banner ads or buttons to unwanted links. Many times you can also customize those to be less conspicuous.

If you feel confident with your web-building knowledge and programming skills, freebies probably aren't for you. Either way, viewers will enjoy using your interactive elements regardless of how they're implemented. 🌐



Elevate is produced exclusively for New Horizons Computer Learning Centers, Inc.



Copyright

© 2009 Eli Journals. This work is an independently produced publication of Eli Research, the Content of which is the property of Eli Research or its affiliates or third-party licensors and which is protected by copyright law in the United States and elsewhere. The right to copy and publish the Content is reserved, even for Content made available for free such as sample articles, tips, and graphics, none of which may be copied in whole or in part or further distributed in any form or medium without the express written permission of Eli Research. Requests for permission to copy or republish any Content may be directed to Mark Lydard at (800) 508-1316.

Interested in a custom-content publication? Email us at customcontent@elijournals.com.