

## Internet Privacy Advocate

[Home](#)[Protect Your Personal Info](#)[Prevent Spam](#)[Protect Your Domain Name](#)

### Welcome to the Network Solutions Internet Privacy Web Site

#### Protecting Your Privacy and Domain Name

The personal data that you provide when you register a domain name should be just that – personal. That's why Network Solutions® is leading efforts in campaigning for stronger Internet privacy regulations and creating tools to help you protect your personal information and online investment.

Take a moment to explore this site and learn more about personal privacy and domain name security, and what you can do to protect them.

[Protect your personal information](#)

[Prevent spam](#)

[Protect your domain name](#)

#### What You Can Do to Protect Your Online Privacy

##### Give Feedback to ICANN

[Send an E-mail](#)

##### Update Your Account

[Review Your Contacts](#)

[Remove Yourself From the Bulk List](#)

[Turn On Domain Protect](#)

[Turn On Auto Renew](#)



## Internet Privacy Advocate

Home

Protect Your Personal Info

Prevent Spam

Protect Your Domain Name

### Protect Your Personal Info

#### Domain Name Contact Information Is Public Information

When you register a domain name, current regulations require that the contact information for your account be included in a public database known as WHOIS.

#### WHOIS Topics

[Why and how is my domain information made public?](#)

[What information is made public?](#)

[How can my information be abused?](#)

[What you should know](#)

[Take a poll and see what others are saying](#)

#### Why and How Domain Is My Information Made Public?

The Internet Corporation for Assigned Names and Numbers (ICANN), the nonprofit regulatory body responsible for accrediting domain name registrars, requires your domain name provider (Network Solutions®) to make your contact information publicly available.

WHOIS information is used in several ways:

Registrars (domain name providers) use it to validate requests to transfer the domain name to another owner or registrar.

Individuals and businesses use it to learn when their own domain is due for renewal or find out when a domain name they want is due to expire.

Law enforcement agencies use it for investigations into illegal activities on the Internet.

Intellectual property right holders use it to pursue those who violate their rights.

[Back to Top](#)

#### What Information Is Made Public?

WHOIS is a public database that includes information about all individuals and businesses that register Internet domain names. The WHOIS database includes the following information:

Domain name holder's name and address

Address, phone number, and e-mail address of the domain name Account

Contacts

Date of the domain name registration

#### What Network Solutions is doing

[Secure online WHOIS search](#)

[Tool to manage your WHOIS contacts](#)

[Leader in efforts to eliminate Bulk WHOIS](#)

#### Actions you can take

[Select contact information to appear in WHOIS](#)

[Opt out of Bulk WHOIS](#)

[Support the Network Solutions proposal to eliminate distribution of Bulk WHOIS](#)

Page scrolls down for more content; see Word file for complete content

## Prevent Spam

### You Can Decrease Spam

Join Network Solutions® in taking steps to reduce the amount of spam that arrives in your e-mailbox.

### Spam Topics

[What is spam?](#)

[How do spammers get my e-mail address?](#)

[What is Network Solutions doing to stop spam?](#)

[Take a poll and see what others are saying](#)

### What Is Spam?

Spam generally refers to commercial e-mail messages sent to e-mail lists that are obtained without the permission of the recipient. These solicitors make money by sending out millions of e-mail messages, even though only a small number of recipients respond to the offers. Common types of spam include work-at-home offers, weight loss programs, credit repair or loan scams, and pornography.

[Back to Top](#)

### How Do Spammers Get My E-mail Address?

Spammers obtain e-mail addresses in many ways, but the most common method is by "harvesting" addresses from the Internet. Sources include public chat rooms and message boards, and databases such as the public [WHOIS](#) information for domain name holders. In addition, many spammers attempt to generate names at random, targeting the largest residential e-mail providers such as AOL, MSN, AT&T, Yahoo!, Juno, and Hotmail.

Internet users may also expose their address inadvertently. Many sites request e-mail addresses, and users may give permission to use and distribute that e-mail address without realizing it. Once your e-mail address gets on a single "opt-in" list, it's only a matter of time before spam arrives in your e-mailbox.

■

[Back to Top](#)

### What Is Network Solutions Doing to Stop Spam?

Network Solutions has taken a leadership role in stopping spammers. Our efforts include limiting mass outgoing messages and working with law enforcement and FBI officials to identify and stop spam. As a Network

### What Network Solutions is doing

[Providing spam protection for e-mail customers](#)

### Actions you can take

[Protect your e-mail address](#)

[Use multiple e-mail addresses](#)

[Choose your e-mail address wisely](#)

[Avoid using auto-responders](#)

[Filter spam](#)

[Report spam](#)

[Create disposable addresses](#)

↓  
Page scrolls down for more content; see Word file for complete content

## Protect Your Domain Name

### Your Domain Name May Not Be As Secure As You Think

Deceptive practices involving domain names are an increasing concern for domain name owners and users. Several recent incidents have been well publicized in which domain names were unknowingly and illegally transferred to another registrar.

### Domain Name Security Topics

- [How could my domain name be at risk?](#)
- [What are unauthorized transfers?](#)
- [What is domain name hijacking?](#)
- [What is domain name squatting?](#)

### How Could My Domain Name Be at Risk?

With common dot-com names in short supply, hijackers and slammers actively seek out domain names that are popular or are nearing renewal. Easily-guessed or shared passwords can place your domain name at risk of hijacking and/or unauthorized transfer.

[Back to Top](#)

### What Are Unauthorized Transfers?

Domain names can be switched or transferred from one registrar to another without the knowledge or consent of the domain name holder. This practice is known as slamming, or unauthorized transfers.

Unauthorized transfers may occur when domain name resellers submit unauthorized transfer requests that, unless stopped by the customer, result in the domain name being transferred to the reseller or to a new registrar. As a result, customers lose the ability to manage and obtain customer support for the affected domain names. Unauthorized transfers often cause services, such as e-mail and Web sites that are associated with those domain names, to be lost or deleted.

■

[Back to Top](#)

### What Is Domain Name Hijacking?

While unauthorized transfers ("slamming") refer to transferring a domain name from one registrar to another, domain hijacking involves picking up a domain name immediately after it expires in order to direct traffic to a new site. Hijacking most often occurs when a domain name holder inadvertently neglects to renew the domain name.

### What Network Solutions is doing

[New domain name security feature](#)

[New domain name auto-renew feature](#)

[Participant in the Uniform Dispute Resolution Process](#)

### Actions you can take

[Lock your domain name](#)

[Renew early](#)

[Use a complex password](#)

[Restrict access to your account](#)

[Ensure contact information is accurate](#)

[Carefully review information about your domain services](#)

↓  
Page scrolls down for more content; see Word file for complete content