



End Stage Renal Disease National Coordinating Center (ESRD NCC)

Introduction to the Internet

Lesson 2: Staying Safe Online



Lesson 2: Staying Safe Online

In this tutorial, you will learn:

- Common privacy and safety terms used on the Internet
- How to locate and understand a website's privacy policy
- About scams and frauds that can be threat to your safety
- Tips you can use to keep your personal information safe online



Common Privacy and Safety Terms

Common Terms

- Some common terms related to Internet safety are:
 - Cookie
 - Malware
 - Virus
 - Encryption
 - Uniform Resource Locator (URL)
- You will learn about each of these terms on the following slides

Cookie

- A **cookie** is a small amount of data sent to your computer by a **website** and saved by your **web browser**
 - Cookies are used to remember information about you
- Cookies serve many purposes, such as:
 - Recording webpage visits
 - Storing preferences, such as custom text size
- While cookies have many functions, their most common use is to store **login** information for a specific site

Malware

- **Malware**, or **malicious software**, is any program or file that is harmful to a computer or computer user
- Types of malware include computer viruses, worms, ransomware, and spyware
- Criminals use malware programs to do things like steal or delete a person's data, or to monitor a person's computer activity without their permission

Virus

- A computer **virus**:
 - Is a program that is usually disguised as a non-harmful program or file
 - Causes harm by inserting itself into other programs or blocking you from opening your computer files
 - Can be spread to your computer by downloading a file from an unsecure website, or by opening an infected file sent to you in an email
- A computer with a virus is commonly called “**infected**”

Encryption

- **Encryption** is the process of encoding text or data files, causing them to be unreadable
- Files that are **encrypted** show a random, scrambled set of letters and numbers instead of text
- A **decryption key** is required to decode encrypted files and return them to a readable form



Uniform Resource Locator (URL)

- Every website has a unique **web address**, also known as a **URL**
- U.S.-based web addresses usually:
 - Start with “www,” which stands for World Wide Web
 - End with a dot followed by some letters that indicate the type of website it is:
 - **.com** indicates a commercial enterprise or business
 - **.org** indicates a non-profit organization
 - **.edu** indicates an educational institution
 - **.gov** can only be used by a government agency
 - **.mil** can only be used by a military agency
 - **.net** is another indicator of a commercial enterprise or business



Staying Safe and Protecting Privacy Online



Internet Safety and Privacy

- When using the Internet, “**safety first**” is a good motto
 - You don’t need to worry about every search or mouse click, but you should take steps to ensure your safety
- Safety online begins with **protecting your privacy**
 - When you visit a website, you have a right to know:
 - ***What***, if any, information you provide is being ***collected***
 - ***How*** any information collected is ***used***
- A website’s **Privacy Policy** will tell you the answers to those questions

Privacy Policy



A **Privacy Policy** (Privacy Notice) will generally be found at the bottom of the home page. It:

- Outlines a website's plan to protect the information of its customers
- Describes how an organization collects, processes, and uses information provided by its customers

A screenshot of the ESRD NCC website. The page is titled "ESRD-Related Grants" and contains several sections: "Grant Sources", "Examples of Assistance", "Application Example", "Application Preparation", and "Writing Resources". On the right side, there is a "Patient Grant Library" sidebar with a list of categories including "ESRD-Related Grants", "Crowdfunding and Social Media", "Unique or Talent-Based Grants", "Government Grants", "Browse a Catalog of Grants", "Scholarships", and "Fraud Awareness". At the bottom of the page, there are three columns of links: "Patients" (Starting Treatment, Treatment Choices, Access Monitoring, Living with Dialysis, Taking Care of Your Mental Health, Community, Emergency Planning, Infection Prevention), "Professionals" (About the Networks, Vascular Access Management, Patient Engagement, Healthcare-Associated Infections, Emergency Preparedness, Patient Education, Quality Incentive Program, Care Transitions, Quality Improvement, Fistula First), and "Resources" (Patients, Professionals, Lifeline for a Lifetime, Emergency Preparedness, Healthcare-Associated Infection (HAI) LAN, Additional Resources, AIM-Specific Resource Libraries, CMS Quality Conference). A red arrow points from the "Privacy" link in the footer to the "Privacy Policy" text in the main content area.

Information Collection

Websites usually collect two types of data:

- **Personally Identifiable Information (PII)**, which can be used to identify, contact, or locate an individual

For example, your:

- Name
- Email address
- Social security number

- **Generic or General Information** about your website visit.

For example, the:

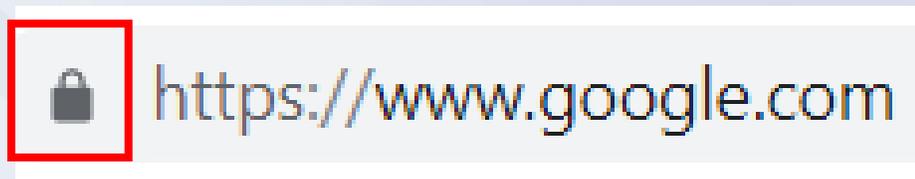
- Date and time of the visit
- Web pages visited
- Type of computer and browser used
- Search engine and key words used

Website Registration

If you've decided that a website is safe, you may be asked to **register** on the site.

- This means you can create an account, or a **login**, for that website with a **user name** and **password**.
 - Logins and passwords protect your data *and* allow a site to collect information.

Important Note: Before you enter any information to create your account, make sure that the sign-up page is secure. This is usually indicated by a **lock symbol** next to the URL that looks like this:





Login Information: User Name

Your user name:

- Can be whatever you want it to be, but not too obvious
- Should be easy for you to remember
- Should be difficult for others to associate with you, such as your name with a series of random numbers that follow

Note: A website may already have someone registered with the user name that you want to use. In that case, you will have to modify or change your user name.



Login Information: Password

- A **password** is the second part of your Login information
- Passwords are the “key” to any online account
- Like a user name, a password should be easy for you to remember but hard for someone else to guess
 - Avoid using common information in your password, like your name, your pet’s name, or your child's name
- Many websites require that passwords have at least one upper case letter, lower case letters, and special characters, like an asterisk, exclamation point, or dollar sign



Threats to Privacy and Security

Online Dangers

- Most computer threats take the form of programs such as malware, spyware, viruses, and/or ransomware
 - These programs can:
 - Take your passwords, personal and/or financial information
 - Lock your computer and demand money, or a ransom, from you
 - Delete your personal data
 - Slow down your computer
- Understanding what computer threats are and how they work is an important part of staying secure
 - The following slides explain different kinds of dangerous online threats and programs and how they work

Spamming

Spamming is a threat that uses messaging systems, such as email, to send:

- Unsolicited messages (“**spam**”)
 - “Unsolicited” means that the recipient has not granted verifiable permission for the message to be sent
- Many bulk messages to large numbers of people from one email address

Note: A message is spam only if it is both unsolicited and bulk



Phishing: What It Is

Phishing attacks are threats that:

- Are used to get your personal and financial information, such as passwords and/or credit card numbers
- Use fake email addresses, websites, or social media sites information that look like real emails and websites from companies you know

Phishing: What to Do

- If you think you are the victim of a phishing attack:
 - Contact the real company directly using contact information provided on an account statement, not information provided in an email
 - Check out the [Anti-Phishing Working Group](#) (APWG) to learn about known phishing attacks and/or report phishing
- Review all URLs carefully to see if they:
 - Go to an unknown website
 - Have a lot of grammar mistakes or spelling errors—This can indicate phishing

Ransomware

- Ransomware is a type of program that, when run, will lock and **encrypt** a victim's computer data, making it impossible to use
- Ransomware involves a demand for a payment to unlock the user's data. Many times, even if the user pays ransom, they are still unable to get their data back
- To avoid ransomware, never open a program sent to you through email. You can install malware detection software to look for files that are infected with ransomware

Fake, Fraudulent, or Scam Websites

Many websites and links look like they are safe There are four simple ways to help figure out if a website is real:

<p>Look at the URL</p>	<ul style="list-style-type: none"> The website name is important <ul style="list-style-type: none"> <i>www.google.com</i> is not the same as www.google.scam-me.com
<p>Look for the Padlock Icon</p>	<ul style="list-style-type: none"> Secure sites will show the padlock icon next to the URL, which tells you the site is secure 
<p>View the Certificate</p>	<ul style="list-style-type: none"> Click the padlock icon to view more security information about the site
<p>Look for Trust Seals</p>	<ul style="list-style-type: none"> Trust seals show that a company has purchased a reputable online security certificate <ul style="list-style-type: none"> Click on a trust seal for more information 



Tips to Stay Protected

- **Keep a clean machine**
 - Keep your computer, as well as smartphones and tablets, up-to-date
- **Use anti-virus and malware detector programs**
 - There are many free options out there!
- **Be aware!**
 - If you get an email from your bank that you were not expecting or an email from a friend with a link in it that doesn't look right, it could be someone trying to get your data
 - When in doubt, don't open the email and delete it right away

Steps for Victims of Online Security Breaches



- **Contact your financial institution immediately** and close the account(s)
- **Watch for any charges** that are not expected
- **Report** security breaches and information theft attempts to your local police department
- File reports with the [Federal Trade Commission](#) and/or the [Internet Crime Complaint Center](#)



Four Steps to Take Quickly

- **Change your passwords**
 - *Do not* use the same password for all online accounts
- **Watch your accounts**
 - Keep track of online, social media, and financial account activity
- **Tell your friends and family**
 - Let them know to look out for strange emails/files that may appear to be from you
- **Scan your computer for viruses and malware**



Activity: Security Smarts Challenge

Lesson 2 Review



Activity: Security Smarts Challenge

1) You should read a website's Privacy Policy because:

- A. It helps you determine if a site is safe
- B. It explains what, if any, information is collected by the website
- C. It tells you how any information collected by the website will be used
- D. All of the above

Go to the next slide to see the correct answer.



Activity: Security Smarts Challenge

1) You should read a website's Privacy Policy because:

- A. It helps you determine if a site is safe
- B. It explains what, if any, information is collected by the website
- C. It tells you how any information collected by the website will be used

Correct

D. All of the above



Activity: Security Smarts Challenge

- 2) Which of the following activities should you be most cautious and careful about when you are online?**
- A. Searching for information
 - B. Giving out your address, phone number, or financial information
 - C. Sending emails to family and friends
 - D. Playing games online

Go to the next slide to see the correct answer.



Activity: Security Smarts Challenge

2) Which of the following activities should you be most cautious and careful about when you are online?

A. Searching for information

 **B. Giving out your address, phone number, or financial information**

C. Sending emails to family and friends.

D. Playing games online.



Activity: Security Smarts Challenge

3) What is the best advice when creating and using a secure password?

- A. Include personal information, like your date of birth
- B. Make it as short as possible
- C. Use the same password across all sites you access
- D. Create a password with both letters and numbers

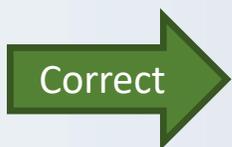
Go to the next slide to see the correct answer.



Activity: Security Smarts Challenge

3) What is the best advice when creating and using a secure password?

- A. Include personal information, like your date of birth
- B. Make it as short as possible
- C. Use the same password across all sites you access



D. Create a password with both letters and numbers



Activity: Security Smarts Challenge

4) How can you catch a computer virus?

- A. Downloading infected software
- B. Opening infected emails
- C. Visiting infected websites
- D. All of the above

Go to the next slide to see the correct answer.

Activity: Security Smarts Challenge

4) How can you catch a computer virus?

- A. Downloading infected software
- B. Opening infected email attachments
- C. Visiting infected websites

Correct

D. All of the above



Thank You!

For additional information, please contact:

NCCinfo@hsag.com

844.472.4250

or visit

www.esrdncc.org