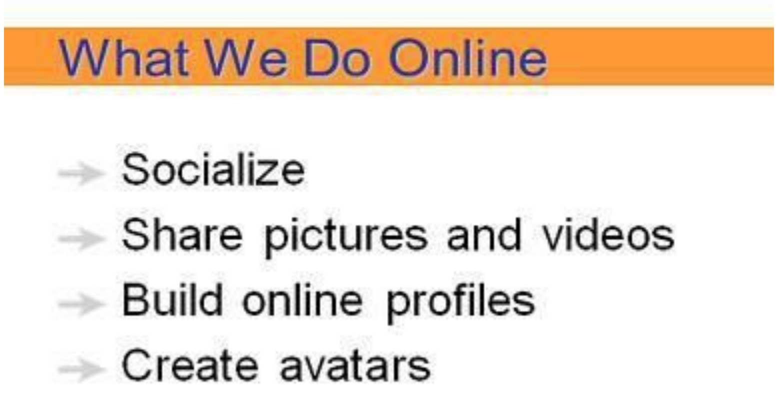
www.kidsactivitydownloads.com

Kids Activity Downloads



What We Do Online

- Socialize
- Share pictures and videos
- Build online profiles
- Create avatars

Download all the available videos if you want to have offline access. Go to on my secure Web download section here:
www.kidsactivitydownloads.com

You can print the page or download the document in the video section here:
www.kidsactivitydownloads.com

An online version of this table of contents for the transcripts here:

Table of Contents

Click on the link for the transcript section you want to view.

Video

1:15 Online Reviews and Recommendations (Video)
3:46 video Protect Your Computer from Malware (Video)
1:41 Sharing Information: A Day in Your Life (Video)
3:51 Net Cetera: Chatting with Kids About Being Online (Video)
0:59 Heads Up: Stop. Think. Click. (Video)
1:02 The Protection Connection (Video)
1:01 Share with Care (Video)
1:20 Stand Up to Cyberbullying (Video)
3:54 Wireless Security (Video)
3:28 Online Shopping Tips (Video)
5:10 Mobile Apps (Video)
3:32 Computer Security (Video)
3:11 Public Wi-Fi Networks (Video)
1:21 Back It Up (Video)
1:37 Hijacked Computer: What to Do (Video)
1:28 Hacked Email: What to Do (Video)

Game

The Case of the Cyber Criminal (Game)
ID Theft FaceOff(Game)
Friend Finder(Game)
Mission: Laptop Security(Game)
Beware of Spyware(Game)
Online Lineup(Game)
Invasion of the Wireless Hackers(Video)
P2P Threeplay(Game)
Phishing Scams(Game)
Auction Action (Game)
Spam Scam Slam(Game)
Follywood Squares(Game)

Tutorial

Invest Quest(Tutorial)
Linksys Router: Change the Default Admin Password (Tutorial)
Netgear Router: Change the Default Admin Password (Tutorial
Apple Airport: Change the Default Admin Password (Tutorial)
Linksys Wireless Network: Set a WPA Password (Tutorial)
Netgear Wireless Network: Set a WPA Password (Tutorial)
Apple Airport Wireless Network: Set a WPA Password (Tutorial)
Linksys Wireless Network: Restrict Access by MAC Address (Tutorial)
Netgear Wireless Network: Restrict Access by MAC Address (Tutorial)
Apple Airport Wireless Network: Restrict Access by MAC Address (Tutorial)
Start the Built-in Firewall in Windows XP (Tutorial)
Start the Built-in Firewall in Mac OS X (Tutorial)
Password Protect Your Computer in Windows XP (Tutorial)

Phishy

Phishy Home 1:00 (Video)

Phishy Office 0:59 (Video)

Phishy Store 1:00 (Video)

Video

1:37 Hijacked Computer: What to Do (Video)

You can't turn your computer on or off. It's acting up, running slow, opening pages you didn't click, and displaying pop-ups constantly. There's a good chance your computer's been hacked or infected with a virus and needs your help.

Stop shopping, banking, and entering passwords online until your computer is cleaned and restored. It's inconvenient to be sure, but it's a necessary step to prevent the situation going from bad to worse, from hack to horrible.

Update your security software. Install a new version from a reputable company. You can use your phone or another computer to check reviews of security software. Tech blogs and retail sites usually post them.

Choose carefully. Scammers sometimes advertise security software that's malware in disguise. Make your decision, get back online, and download the software. If the security software finds malware, it flags it for you. Delete the suspicious files and restart your computer. If you're still having problems, contact your computer manufacturer or other tech support and find out what else you can do.

Once your computer is back to normal, change the password you've been using for your bank accounts, your email accounts, and all your other important accounts. The safest route is to choose and use passwords that have upper and lowercase letters as well as numbers and symbols.

And finally, make sure your operating system and internet browser are set to update automatically. You want to keep your computer operating at peak performance. Visit onguardonline.gov to learn more.

Back to Top

1:28 Hacked Email: What to Do (Video)

Your friends and family are getting e-mails from you that you didn't send. Or maybe you want to check your e-mail, but wait, you can't login. Sound familiar? Chances are your e-mail's been hacked.

Don't panic. The situation can be fixed. Start by updating or installing security software from a company you can trust. And set it to update automatically.

Hackers often hijack accounts by infecting your computer with malware. So it's important to scan your computer first. Delete anything that identifies as suspicious and restart your computer. Now you're working with a clean slate.

Next, if you can get into your account, change your password. If you use similar passwords for other accounts, change them, too. Passwords are the keys that open your accounts. They have to be memorable for you, but hard for someone else to guess. Some people use software that manages passwords to help create strong passwords and keep track of them.

If you can't get into your account, check with your e-mail provider to find out how to restore it. Once you've got your account back, and check your account settings to make sure no one added any links to your e-mail signature, and that your e-mails aren't being forwarded to someone else.

Finally, let your family and friends know your e-mail was hacked. Think of it as spreading good computer karma. And they may have some work to do, too. Want to know more about protecting your e-mail from hack attacks? Visit onguardonline.gov.

1:21 Back It Up (Video)

From tax forms to family photos, the files on your computer are valuable. If you don’t want to lose them, back them up, and practice good computer security habits to protect yourself from hackers and viruses.

Back to Top

3:28 Online Shopping Tips (Video)

Day by day, more and more people are shopping online. It’s convenient, and you can bring a world of choices to your computer, phone or tablet.

Are you one of the millions of people looking to buy something online? If you are, there are steps you can take to avoid hassles, get the right product at the right price, and protect your financial information.

First, plan ahead by setting a budget. Ask yourself, “How much do I want to spend?” Be sure to include delivery costs in your budget.

Second, determine what’s most important to you about the item you’re thinking about buying. What are the “must-have” product features? Are there features that would be nice to have, but you can live without? This will help you choose the product that meets your needs.

Take a few minutes to compare products. Type the name into a search engine along with words like “review,” “complaint” or “scam.”

Read online reviews from other people who bought the item or from product experts. Look for feedback about how well the product works and its overall quality.

If you’ve never heard of the company selling the product, look for reviews about their reputation and customer service. Read a few reviews so you’re not relying on just one source.

Of course, you’ll also want to know the total cost of the product.

Check shopping comparison sites to compare the price of the product at different websites. Remember, shipping costs and other “add-ons” may not be included in these prices. Look for online coupon codes. Search the store’s name with terms like “coupons,” “discounts,” or “free shipping.”

Before you decide where to buy, check out the terms of the deal. When will you get your order? The law requires sellers to ship items within 30 days of the sale. If you have to return the item, can you get a refund? Who pays for return shipping? Is there a restocking fee?

Next, decide how to pay.

Paying by credit card gives you some protections that other methods of payment may not. If there's a problem, the law gives you the right to dispute charges and temporarily withhold payment while your dispute is investigated. If someone uses your credit card without your permission, some companies will cap your liability at $50. Others will waive the charges entirely.

Before you enter your credit card or other financial information online, check if the website address starts with "https". The "s" stands for "secure" and means that your information is encrypted before it's transmitted.

Now, you should be ready to enjoy whatever you've bought online. If you have a problem with an online purchase or charge, try to work it out with the seller first.

If you can't resolve the problem, file a complaint with the Federal Trade Commission, the nation's consumer protection agency, at ftc.gov/complaint.

By planning, comparing products and costs, and making sure you check out securely, you can make your online shopping experience safer—and more enjoyable.

Remember: it's easy to find trusted information about online security. Just visit OnGuardOnline.gov, the federal government's site to help you be safe, secure and responsible online.

Back to Top

5:10 Mobile Apps (Video)

The mobile apps market is booming. If you're in the business of developing apps, it's important to know about basic ? and relevant ? consumer protection guidelines.

Hi, I’m Laura Berger, an attorney at the Federal Trade Commission. Whether you run an established company or a start-up, the FTC has suggestions to help you comply with truth-in-advertising standards and privacy principles. Every app is different. But there are some general guidelines to consider if you’re developing an app.

Truth in advertising is simple: Tell the truth when you’re talking about your product.

Once you start distributing your app, you’re an advertiser. An ad isn’t just a multi-million dollar TV spot or global marketing campaign. It’s pretty much anything a company tells a prospective customer about what a product can do. This could be on a web site, in an app store, or even a feature–like a privacy setting or control – that you built into the app itself.

One rule of thumb is to look at your product and your advertising from the average user’s perspective. And if you make objective claims about your app, you need solid proof to back them up before you start distributing it.

When it comes to disclosures, display key information about your product clearly and conspicuously. Generally, the law doesn’t dictate fonts or type size. But the FTC has taken action against companies that have buried important terms in long licensing agreements, in dense blocks of legal mumbo jumbo, or behind vague hyperlinks.

This makes good business sense, too. It shows people that you aren’t trying to hide anything in the fine print.

Now, moving on to privacy: Practice “Privacy by Design”. This means incorporating privacy considerations from a product’s concept stage to its launch and updates. Build privacy protections into development, limit the information you collect, securely store what you hold onto, and safely dispose of any data you don’t need. Think through your default settings with an eye toward privacy. If you’re collecting or sharing information in a way that people wouldn’t expect, get their express permission first.

Be transparent about your data practices. If you need to collect user information for the app to work, be clear about what information you collect and what you do with it.

Give users a choice when it comes to privacy. Privacy settings, opt-outs, or other tools let users control how their personal information is collected and shared. Make it easy for people to find the tools you offer and design them so they're simple to use.

Honor your privacy promises. Chances are you've told users about your security standards or what you do with their personal information, whether that message is in your privacy policy or somewhere else. App developers – like all other marketers – have to live up to their privacy promises. What if you decide to modify your privacy practices sometime down the road? Get users' affirmative permission for material changes.

If your app is designed for kids ? or if you know that you collect personal information from kids ? you might have additional requirements under the Children's Online Privacy Protection Act and the FTC's COPPA Rule. Under COPPA, any company whose app is directed to users under 13 or who knows that a user is under 13 must clearly explain its information collection practices. In addition, COPPA requires you to get parental consent before the app collects any personal information from a child and requires that you keep a kid's personal information confidential and secure. Visit the Business Center for compliance advice.

Even when you're not dealing with information from kids, it's smart to get a user's sign-off before you collect sensitive information. What do we mean by "sensitive"? Medical, financial or geo-location information come to mind as examples.

And finally, keep data secure.
- Collect only the information you need.
- Take reasonable precautions against well-known security risks.
- Limit access to data to a need-to-know basis. And
- Safely dispose of data when you no longer need it.

That's the download on mobile apps. If you want to learn more, read Marketing Your Mobile App: Get It Right from the Start, available at business.ftc.gov.

Back to Top

3:32 Computer Security (Video)

Every day, you hear about scammers, hackers, and thieves…

…trying to use the internet to steal your money and your financial information.

The fact is– you, me—we—can foil many of their attempts. Every day we do things to make it tough for bad guys to break into our homes and our cars. We can make it tougher for them to break into our computers, too.

Here are some way to foil a hacker and protect your financial information:

1. Install security software on your computer.

Well-known companies offer plenty of free options.

Set the software to update automatically so it can deal with any new security threats.

While you're at it, set your operating system and web browser to update automatically, too.

If you're not sure how, use the help function and search for "automatic updates".

If you get a phone call, an email, a text, or a popup that says your computer has a virus or malware, don't buy the story--

--or the security software they're selling. It could be a trick…

… to get you to buy software that's worthless, or even harmful.

2. Treat your financial information like cash. It's a hot commodity. If someone asks for

your financial information--

--say your Social Security, credit card, or bank account number—ask why they need it and how they're going to protect it.

3. If you think you've found a good deal online,

But you aren't familiar with the company,

Dig a little deeper.

A quick internet search with the name of the company…

… and the word "review" or "complaint" can reveal a lot.

Always look for a physical address and phone number, too. That way you know who to contact if there's a problem.

4. Don't provide your personal or financial information unless the website you're on is secure. If the URL doesn't start with https, don't enter your financial information. That S stands for secure. It means the information you're sending is encrypted and protected.

5. Make your passwords count. They should be at least 10 characters—and a mix of numbers, letters and special characters.

Don't use your name, birth date or common words.

Don't use the same password for several accounts, as tempting as that may be.

If it's stolen, hackers can use it to access your other accounts. Keep your passwords in a secure place, and don't share them with anyone.

6. Back up your computer files. For example, copy important files to an external hard drive on a regular basis. That way, if there's a problem with your computer, you won't lose everything.

Life is online. Whether you live it using a smart phone, a tablet, a laptop, or a desktop, it's a good time to make computer security a habit.

Find out more at OnGuardOnline.gov, the federal government's site to help you be safe, secure and responsible online.

Back to Top

3:11 Public Wi-Fi Networks (Video)

Many hotels…

… coffee shops…

… airports and other places offer free Wi-Fi hotspots. They're convenient. Unfortunately, they often aren't secure.

That could make it easy for someone else to access your online accounts or steal your personal information. So, what can you do to reduce your risk?

Encryption is the key to keeping your information secure online. When information is encrypted…

… it's scrambled into a code so others can't get it.

How can you be sure…

… your information is encrypted?

Two ways: one, use a secure network to access the internet.

Don't assume that a public Wi-Fi network uses encryption. In fact, most don't. You can only be sure that a network uses effective encryption if it asks you to provide a

WPA or WPA2 password.

If you aren't sure, it's best to assume the network is not secure.

The second way to protect your information is to send it through a secure website.

A secure site will encrypt your information—even if the network doesn't.

If the web address starts with "https," then your information is encrypted before it's sent. The "s" stands for "secure." Look for the "https" on every page you visit, not just when you log in.

If you use an unsecured Wi-Fi network to login to an unencrypted website.

.. strangers using that network can hijack your account and steal your private documents, contacts, family photos--

Even your user name and password. If that happens, an imposter could use your e-mail.

.. or social networking account to pretend to be you and scam people you care about.

Or a hacker could use your password from one website to try to login to…

… a different account and access your personal or financial information.

Here are some steps you can take to protect yourself when you use a public Wi-Fi hotspot:

- Only log in or enter personal information on secure sites that use encryption. Again, look for a web address that begins with "https"

Don't use the same user name and password for different sites. It could give someone who gains access to one of your accounts access to many of your accounts.

Never email financial information…

… including credit card, Social Security, and checking account numbers, even if the network and website are secure.

Don't stay permanently signed in to accounts.

When you've finished using a site, log out.

The bottom line? Secure Wi-Fi hotspots require a password. Secure websites start with https.

And remember: it's easy to find trusted information about computer security. Just visit OnGuardOnline.gov, the federal government's site to help you be safe, secure and responsible online.

Back to Top

1:15 Online Reviews and Recommendations (Video)

[music playing with no voice over]

Text on screen:

An Important message from the Federal Trade Commission

Whether you're looking for a hotel

or searching for a new pair of shoes

you probably turn to the internet for customer reviews

from "five stars", "likes", "thumbs ups", or "must buys" –

a positive opinion could impact your decision to buy it or try it.

while blogs, websites, and social networks are great resources –

you may not be getting the whole story.

for example,

your Facebook Friend, who gushes about how a new dog food,

may be receiving a free dog food in exchange for her glowing review

or the hotel, with the five star rating

might have paid a blogger to write a stellar review

while the law says that reviewers should disclose their connection to the company

not all of them do.

it can be difficult to tell if the reviewer has a connection to the company

So, before you buy anything based on a review...

Do an internet search,

Look for credible opinions from trusted sources,

Compare reviews from a variety of websites

In the end, it pays to learn as much as you can.

To learn more... OnguardOnline.gov/shopping

Back to Top

3:46 Protect Your Computer from Malware (Video)

Would it surprise you to learn that millions of computers in the US are infected with malware? That's a lot of computers. So what's malware, and why should you care?

Malware, short for malicious software, includes viruses and spyware that get installed on your computer or mobile device without you knowing it. Criminals use malware to steal personal information and commit fraud. For example, they may use malware to steal the login information for your online accounts or to hijack your computer and use it to send spam. An infected computer can lead to serious problems, like identity theft.

The good news, there's a lot you can do to protect yourself and your computer. One of the most important steps you can take, install security software from a reliable company and set it to update automatically. The bad guys constantly develop new ways to attack your computer, so your software must be up to date to work.

Set your operating system and your web browser to update automatically too. If you're not sure how, use the help function and search for automatic updates. Don't buy security software in response to unexpected calls or messages, especially if they say they scanned your computer and found malware. Scammers send messages like these to trick you into buying worthless software, or worse, downloading malware.

What else can you do? Use a pop up blocker, and don't click on links and popups. Don't click on links or open attachments in emails unless you know what they are, even if the emails seem to be from friends or family.

Download software only from websites you know and trust. Free stuff may sound appealing, but free downloads can hide malware. Make sure your web browser's security setting is high enough to detect unauthorized downloads. For example, use at least the medium security setting.

Even if you take precautions, malware can find its way onto your computer. So be on the lookout for these signs. Your computer runs slowly, drains its battery quickly, displays unexpected errors or crashes, it won't shutdown or restart, it serves a lot of popups, takes you to web pages you didn't visit, changes your home page, or creates new icons or toolbars without your permission.

If you suspect malware, stop doing things that require passwords or personal info, such as online shopping or banking. Use a different computer, maybe one at work or at your local library, to change your passwords. Update your security software and run a system scan. Delete files it flags as malware.

If you can't fix the problem on your own, get help from a professional. Your computer manufacturer or internet service provider may offer free tech support. If not, contact a company or retail store that provides tech support.

Keep in mind, the most important thing you can do to prevent malware is to keep your computer software up to date. And remember, it's easy to find trusted information about computer security. Just visit onguardonline.gov, the federal government site to help you stay safe, secure, and responsible online.

Back to Top

1:41 Sharing Information: A Day in Your Life (Video)

Every day you take advantage of all kinds of services mobile, social media, free internet search and more.
When you use these services, you're sharing information about yourself.
With friends, With businesses, While you're out and about, While you're at home.
That information is shared and sold.
Within Businesses, With their Affiliates, With Ad Networks.
So, in a typical day, you might shop at a store and use a loyalty card to take advantage of a sale, and your shopping habits may be shared or sold.
You might need to fill a prescription and your prescription history may be shared or sold.
You might use a daily coupon app to get a deal at a nearby restaurant and your location information may be shared or sold.
You might visit a news site where you notice an ad for your favorite brand of shoes. It's an online sale, this weekend only, so you buy a pair.

And the articles you read and your shoe preferences may be shared or sold.
You might login to a social network and see that your friends are filling out an "All About Me" quiz.
You get the quiz app and share your answers, and your quiz responses and profile information may be shared or sold.
A regular day. You've taken care of business, used some free services, gotten some good deals and revealed all kinds of information about yourself.
So at the end of the day, the question is, Who has your information and where is it going next?

Back to Top

3:51 Net Cetera: Chatting with Kids About Being Online (Video)

The internet. It offers enormous opportunities to communicate!

Most of us – including kids – do all kinds of things online. We connect through email, text and instant messaging. We post and distribute pictures and videos.

We may have profiles on social networks, where we share our lives, our plans and our thoughts with hundreds of people.

These ways of communicating and socializing can be convenient and fun – yet they come with certain risks.

Many parents wonder, “how should I talk to my kids about being safe online?

A booklet called Net Cetera provides some practical tips. It’s based on the idea that the first step to protecting kids online is more about talking than technology.

When kids want important information, they turn to their parents.

So talk to them about your values – honesty, fairness, courtesy, or whatever values are most important in your family – and how they apply in an online setting.

By communicating your values and expectations, you'll help your kids make smarter, more thoughtful decisions when they face tricky situations online.

Here are some things to talk about:

Social Networking sites, chat rooms and blogs are some ways kids socialize online. They can help kids connect with friends, but it's important to help your children learn how to navigate these spaces safely.

Among the pitfalls: sharing too much information, and posting pictures or video that can hurt someone's feelings or damage a reputation.

Talk to your kids about applying good judgment to help minimize those pitfalls.

Most mobile phones have cameras and can shoot video, making it easy for teens to capture and share every moment on the go.

Encourage kids to think about their privacy and that of others before they share photos and videos.

Cyberbullying is bullying that happens online – and it's a lose-lose proposition.

It makes the person being harassed feel bad – and it makes the bully look bad.

Talk to your kids about treating others with respect, and let them know they can talk to you if someone harasses them.

If that happens, encourage your kids to block the bully if they can, and ignore him or her if they can't. That's because bullies are looking for a reaction.

If it continues, ask your kids to save the evidence and share it with you or another adult they trust.

Mean behavior usually stops pretty quickly when someone speaks up.

Encourage your kids to stand up for themselves, and to stand up for someone else being cyberbullied.

And talk to your kids about treating others online the same way they want to be treated.

Here are some other tips to keep in mind.

Start early: Young kids see their parents using smart phones and computers. So as soon your kids use one themselves, it's time to talk to them about safety.

Initiate conversations: Don't wait for kids to come to you. Use everyday chances to talk with them: news stories about cyberbullying, a storyline on TV – both can be the start of a good conversation.

Be patient: Most kids need small bits of information repeated – often – for it to really sink in. Keep talking; chances are it'll pay off.

Read Net Cetera for more information about chatting with your kids about being safe online. It's free. And you'll find it at OnGuardOnline.gov.

Back to Top

0:59 Heads Up: Stop. Think. Click. (Video)

We spend a lot of our lives online. We text. We play games. We share photos and video.

And as we do these things, it’s easy to get caught up and not think before we post or click.

It can be easy to over-share, and embarrass yourself, or someone else.

So no matter how fast your fingers fly on a keyboard or cell phone, the best tool you have to avoid risk – is your brain.

So when you’re ready to send a text, or post a picture or video... Stop and think.

Do you want a message or photo you posted to show up years from now, when you apply for college or a job?

While a video or picture may be funny to you, how will other people feel about it?

Being online is part of your life.

So, take a second. Stop and think before you click.

Back to Top

1:02 The Protection Connection (Video)

Since being online is part of our lives, it’s a good idea to take steps to protect ourselves, our information, and our computers.

One thing you can do to stay safe is to limit your online friends to people you actually know.

By turning on privacy settings and learning about location-based services, you can keep strangers from learning too much about you.

And don’t give certain information out - to anyone. Your Social Security number, family bank accounts, and even your password can cause lots of trouble in the wrong hands.

You can protect yourself and your computer by keeping up-to-date on security software and being cautious about what you click. Emails, P2P downloads, and promises of 'free' stuff can hide viruses and spyware.

Being online is part of your life, So stop and think before you click.

Back to Top

1:01 Share with Care (Video)

Being online is a great way to share information and connect with friends. But it’s important to remember that the things we post online can affect people in the real world.

Before you post anything online, ask yourself a few questions. How would you feel if your family, your teachers, your coaches, or your neighbors found it?

Even if you turn on privacy settings, it's impossible to completely control who sees what you post. Or when.

Do you want a message or photo you posted to show up years from now, when you apply for college or a job?

Once you post information online, you can't take it back. Even if you delete it, it can still live somewhere else.

While a video or picture may be funny to you, it may be embarrassing or hurtful for someone else.

Being online is part of your life, so stop and think before you click.

Back to Top

1:20 Stand Up to Cyberbullying (Video)

We spend lots of time online. We text, we comment, we share. It’s a big part of our lives.

But communicating with someone online is just like talking to them in real life.

Everyone appreciates politeness and no one likes it when people make fun, or spread gossip, rumors or lies.

The fact is that some people do try to hurt others online.

It’s called – cyber bullying – and it’s a lose-lose situation:

It makes the person being harassed feel bad – and it makes the bully look bad.

It might lead to trouble with school authorities or even the police.

If someone is harassing you online, it’s important not to respond.

That’s because bullies are looking for a reaction. Block them if you can, ignore them if you can’t.

If it continues, save the evidence and ask an adult for help.

And don't be afraid to stand up for yourself, or to stand up for someone else being cyber bullied.

This behavior usually stops pretty quickly when someone speaks up.

And when you’re communicating online – remember to treat people the way you’d like to be treated.

Know how to handle yourself, because being online is part of your life.

So stop and think before you click.

Back to Top

3:54 Wireless Security (Video)

A wireless network is something that lets your computer access the internet without using any wires or cables. So if you have a wireless network at home, you probably have a device called a wireless router which transmits data to your computer remotely.

The biggest benefit to using a wireless network is convenience. It lets you move around and work on a laptop anywhere in your house or in your business and you can also connect different computers to the internet without having to deal with the big tangle of messy wires.

Unless you take a few basic steps to protect your wireless network, anyone with a wireless ready computer can use your network without your permission. This is something that we call piggybacking.

Now in most cases the only harm you might actually experience is a slowing down in your broadband speed as different people try to share one network connection. But in other cases a hacker could access the personal information that is stored on your computer and if someone uses your network to commit a crime or send spam, that activity could be traced back to your account, so you definitely want to be careful.

To protect yourself when your on the wireless network you can do a few things...

First you want to make sure that your router isnt broadcasting the presence and identity of your wireless network. If your router is publicly broadcasting, it can make it easier for hackers to find and access your network. Instead you want to hide your wireless network by turning off the identifier broadcaster feature on your router.

Another thing you can do is to not use a default name or identifier that came with your router. Using the default identifier makes it easier for hackers to find and access your network. Instead you want to change the identifier for your router to a unique name.

Now the best way to secure your wireless network is to turn on the encryption feature on your router. This will make sure any data sent over the network is encrypted or scrambled.

Now there are different kinds of encryption standards that you can use in your home wireless network. The strongest one is something called WPA2 and the weakest one is called WEP. Now of course we recommend you use the strongest encryption standard that you can.

And one thing that alot people dont realize is that when you buy your router, its often sold with the encryption feature turned off. So one thing that you definitely want to do is make sure your router has encryption turned on. And you can do this by following the directions that come with your router, but if your like me and you throw away your instructions and packaging as soon as you get your gift, you should be able to get the directions from the website of the company that manufactured your router.

Now every router comes with a preset password for changing the administrative features on your router. One thing you want to do is change the password to something only you would know. The longer the password, the tougher it is going to be to crack so we recommend using a password that has at least twelve characters.

Another step you can take is to restrict access to your wireless network to specific computers that you know are safe. Every computer that can communicate with the network is assigned its own unique media access control address, or what we call a MAC address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access the network. To learn how to do this just go to the OnGuard Online website.

And finally when your outside in a public place, you don’t want to assume that public wireless networks are going to be secure. I'm talking about all those WiFi hotspots that you find in cafes and libraries, hotels, universities, and tons of other public places. You should always keep in mind that any information you send or receive over a public wireless network could be seen by other people.

And if you want more tips and video tutorials on securing your wireless network, come visit us at Onguard Online at OnguardOnline.gov/wireless.

Back to Top

The Case of the Cyber Criminal (Game)

A techie spy and his cunning crew are out to get your personal information. Stop them cold by proving you're ready to protect yourself online.

ID Theft FaceOff (Game)

Your identity's been stolen! Luckily, this time you just need to correctly answer some questions on protecting your identity to get it back.
Compete with our contestants for a spot on the Friend Finder All-Star List. Earn your spot by showing you're savvy when it comes to making friends online.

Friend Finder (Game)

Compete with our contestants for a spot on the Friend Finder All-Star List. Earn your spot by showing you're savvy when it comes to making friends online.

Back to Top

Mission: Laptop Security (Game)

You've already lost one laptop, Agent Smith. Your job's on the line if it happens again. Make wise choices this time, and it's mission accomplished.

Beware of Spyware (Game)

Protect your computer from spyware and viruses that can cause it to run slowly or give fraudsters access to your personal information.

Online Lineup (Game)

Are you a shrewd online shopper who can spot a risky offer? Peruse our sales pitches to find out. You decide who gets your business and who gets the boot.

Invasion of the Wireless Hackers (Game)

Hackers hunting for vulnerable wireless networks are closing in. Stop the hack attack with correct answers to these wireless security questions.

P2P Threeplay (Game)

Dare you take on the Great and Powerful P2P Master? A game of tic-tac-toe awaits anyone willing to test their peer-to-peer file-sharing smarts.

Back to Top

Phishing Scams (Game)

Phishers are looking to lure you with bogus emails and pop-ups that seem safe. Will you take the bait or live to swim another day?

Auction Action (Game)

Congratulations! You're the next contestant on AuctionAction, the game that puts your online auction know-how to the test.

Spam Scam Slam (Game)

Three rounds. Three strikes. Make it through this game, and it's clear — you're on to spam scams and not likely to get slammed by the next one.

Back to Top

Follywood Squares (Game)

Match wits with an opponent and an array of guest stars answering questions about health products and information online.

Linksys Router: Change the Default Admin Password (Tutorial)

Step-by-Step Instructions to Change the Default Admin Password on Your Linksys Router

Connect to your wireless network.
Open your Web browser and type in the Web address http://192.168.1.1
Press Enter key
Type in the User Name for your network
Type in the default Password
Press OK button
Select the Administration text link
Type in a new password in the Router Password box, and then reenter it
Click the Save Settings button
Click the Continue button

Developed by the Internet Education Foundation as part of its GetNetWise program.

Back to Top

Netgear Router: Change the Default Admin Password (Tutorial)

Step-by-Step Instructions to Change the Default Admin Password on Your Netgear Router

Connect to your wireless network.
Open your Web browser and type in the Web address http://www.routerlogin.net
Press Enter
The NETGEAR Prompt dialog opens
Click the OK button
Type in the user name and default password (it's probably "password")
The Router Manager window will appear
Under the header Maintenance, select the Set Password menu item
Type in the old, default password (again, it's probably password). And then type in a new password -- twice.
Click the Apply button

Apple Airport: Change the Default Admin Password (Tutorial)

Step-by-Step Instructions to Change the Default Admin Password on Your Apple Airport Base Station

NO TRANSCRIPT

Back to Top

Linksys Wireless Network: Set a WPA Password (Tutorial)

Step-by-Step Instructions to Set a WPA Password on Your Netgear Wireless Network

In your web browser, type in the address http://www.routerlogin.net. Press Enter.
When the NETGEAR prompt dialogue box appears, type in your User Name and Password. Click OK.
The Router Manager window will appear. Click on Wireless Settings. Type in your User Name and Password. Press Enter.
Under Security Options, click the WPA-PSK button.
Select the Passphrase text box, and type in a passphrase. Click Apply.

Developed by the Internet Education Foundation as part of its GetNetWise program.

Back to Top

Netgear Wireless Network: Set a WPA Password (Tutorial)

Step-by-Step Instructions to Set a WPA Password on Your Linksys Wireless Network

Connect to your wireless network.
Open your Web browser and type in the Web address http://192.168.1.1
Press Enter key
Type in the User Name for your network
Type in the Password
Press OK button
Select the Wireless text tab
Select the Wireless Security text item

Pull down and select the WPA Pre-Shared Key menu item
Pull down and choose the WEP menu item
Type in a good password
Click the Save Settings button

Developed by the Internet Education Foundation as part of its GetNetWise program.

Back to Top

Apple Airport Wireless Network: Set a WPA Password (Tutorial)

Step-by-Step Instructions to Set a WPA Password on Your Apple Airport Wireless Network

Open your AirPort Admin Utility application (this program was installed from the CD-ROM when you set up the device)
Find your network's name and double-click it or press the Configure button on the bottom right of the screen.
Here, our network name is Apple Airport Express
Enter your password and click OK.
The Configure "Apple Airport Express" Base Station should open. Click on AirPort tab.
Click on Wireless Security… button.
Pull down the Wireless Security menu (by clicking on the word Off. Drag your mouse down to WPA2 Personal.
Click on Set Pre-Shared Key… button.
Type in a Pre-Shared Key, then verify it by re-typing it. Click OK.
Click OK again.
Finally, make sure to hit the update button to save the changes.

Developed by the Internet Education Foundation as part of its GetNetWise program

Back to Top

Linksys Wireless Network: Restrict Access by MAC Address (Tutorial)

Step-by-Step Instructions to Restrict Access by MAC Address on Your Linksys Wireless Network

Connect to your wireless network.

Open your Web browser and type in the Web address http://192.168.1.1

Press Enter key

Type in the User Name for your network

Type in the default Password

Press OK button

Select the Wireless text menu item

Click on the Wireless MAC Filter text link

Select the Enable radio button

Select the "Permit only…" radio button

Click the Edit MAC Filter List button

The MAC Address Filter List window opens

Type in your computer's MAC Address in the first open box

Click the Save Settings button

Again, click the Save Settings button

Developed by the Internet Education Foundation as part of its GetNetWise program.

Netgear Wireless Network: Restrict Access by MAC Address (Tutorial)

Step-by-Step Instructions to Restrict Access by MAC Address on Your Netgear Wireless Network

Connect to your wireless network.

Open your Web browser and type in the Web address http://www.routerlogin.net

Press Enter

The NETGEAR Prompt dialog opens

Click the OK button

Type in the user name and default password

The Router Manager window will appear

Under Advanced, select the Wireless Settings menu item

Click the Setup Access List button

Check the radio button next to Turn Access Control On

Click the Add button

The program will display all computers connected to the wireless network -- with its MAC address. The one shown here is ours.

Select the radio button next to your computer's name and MAC address

Click the Add button

Click the Apply button

Developed by the Internet Education Foundation as part of its GetNetWise program

Back to Top

Apple Airport Wireless Network: Restrict Access by MAC Address (Tutorial)

Step-by-Step Instructions to Restrict Access by MAC Address on Your Apple Airport Wireless Network

Open your AirPort Admin Utility application (this program was installed from the CD-ROM when you set up the device)

Find your network's name and double-click it or press the Configure button on the bottom right of the screen.

Here, our network name is Apple Airport Express

Enter your password and click OK.

The Configure "Apple Airport Express" Base Station should open. Click on AirPort tab.

Click on Wireless Security… button.

Pull down the Wireless Security menu (by clicking on the word Off. Drag your mouse down to WPA2 Personal.

Click on Set Pre-Shared Key… button.

Type in a Pre-Shared Key, then verify it by re-typing it. Click OK.

Click OK again.

Finally, make sure to hit the update button to save the changes.

Developed by the Internet Education Foundation as part of its GetNetWise program.

Back to Top

Start the Built-in Firewall in Windows XP (Tutorial)

Step-by-Step Instructions

Through the Start menu select the "Control Panel" menu item.
Select the "Network and Internet Connections" item.
Select the "Windows Firewall" icon.
If it is not already checked, check the "On (recommended)" radio button.
Click the "OK" button to make your firewall active.

Developed by the Internet Education Foundation as part of its GetNetWise program.

Start the Built-in Firewall in Mac OS X (Tutorial)

Step-by-Step Instructions to Start the Built-in Firewall in Mac OS X

Pull down the Apple icon in the top left corner of your Desktop
Select System Preferences from the menu.
Under the category Internet & Network click on the Sharing icon.
Make sure the Firewall tab is selected.
Click the Start button to enable the built-in firewall in your operating system.

Developed by the Internet Education Foundation as part of its GetNetWise program.

Back to Top

Password Protect Your Computer in Windows XP (Tutorial)

Step-by-Step Instructions to Password Protect Your Computer in Windows XP

Click the Start button.
Select the Control Panel menu item.

After the Control Panel window opens, select the User Accounts link.
Make sure to password protect all of your computer user accounts -- especially the Administrator accounts.
Under User Accounts, click the name of a user who is not password protected.
Select the Create a Password option.
Click the text box below Type a new password: and type your password. Then in the box below, re-type the password to confirm, and then below that, type a password hint to help you remember.
Click the text box below Create Password button.
Repeat this process for all your computer's user accounts.

Developed by the Internet Education Foundation as part of its GetNetWise program.

1:00 Phishy Home (Video)

A phisher pays an unexpected visit to someone's home. To learn more, check out Phishing. http://www.onguardonline.gov/articles/0003-phishing

Husband:
Coming….

Man:
Good afternoon Mr. Thomas. I'm from your credit card company. We suspect several unauthorized transactions on your card.

Husband:
Really? My credit card company?

Man:
Yes, and we care about your security, so we make house calls. Good news is, you give me your social security number and we'll take care of you.

Husband:
Is that all you need?

Uh… oh, not quite – we also need your PIN number. I forgot.

Husband:
What's that on your back?
Nothing.

Husband:
Oh, I get it… You're fishing for my personal information right?

Man:
No.

Husband:
So you can steal my identity, right?

Man:
No!

Husband:
Then why do you have a fin sticking out of your back?! Honey, get my tackle box and rod!

Narrator:
Onguardonline.gov has tips to help you be on guard against Internet fraud, to secure your computer, and protect your personal information.
To be more secure online, log onto… Onguardonline.gov. Stop – Think – Click.

Back to Top

0:59 Phishy Office (Video)

A phisher shows that phishing can happen when you least expect it — even at the office. To learn more, check out Phishing.
http://www.onguardonline.gov/articles/0003-phishing

Woman: (gasp)

Man: Sorry about that… I'm here to help.

Woman (nervous):
You are?

Man:
Absolutely. Your bank account information needs to be updated…to be sure that it's not compromised.

Woman:
Really. Compromised? How?

Man:
I need your password – and I need it now.

Woman:
My password? My bank has my password. Something here doesn't seem right.

Man:
What?

Woman:
I can't quite put my finger on it.

Man:
Trust issues, huh? You know, once we figure this whole thing out, maybe we could grab a cup of coffee. If you give me your credit card number I could even order something for us right now… Hi, whoa…

Guard:
You fishing for information?

Man:
Uh, uh…This isn't what it looks like. Ow. Easy on the fin! Ow. Ow!

Narrator:
Onguardonline.gov has tips to help you be on guard against Internet fraud, to secure your computer, and protect your personal information.
To be more secure online, log onto… Onguardonline.gov. Stop – Think – Click.

Back to Top

1:00 Phishy Store (Video)

A phisher visits a clothing store in hopes of getting a shopper's financial information. To learn more, check out Phishing.
http://www.onguardonline.gov/articles/0003-phishing

Man:
Hmm, I think the blouse is more your type

Young Woman:
Really?

Man:
Mm-hmm, but before you try it on, I need to update some account information – just need to verify your credit card numbers.

Young Woman:
My credit cards?

Man:
Uh-huh, And a password or two. Won't take a second.

Young Woman:
Something smells a little fishy around here…

Man:
What makes you say that?

Female Store Clerk:
Looks like he's fishing for your personal information... so he can steal your identity.

Man:
You know that’s insulting? I was trying to help

Female Store Clerk:
Would you look at that! I thought you characters only did your dirty work over the internet…

Man:
Well we do… I mean that we… with the… Gotta go! Oof!

Narrator:
Onguardonline.gov has tips to help you be on guard against Internet fraud, to secure your computer, and protect your personal information. To be more secure online, log onto… Onguardonline.gov. Stop – Think – Click.

Back to Top