

Internet Safety Tip Card

Office of the Attorney General
ERIC T. SCHNEIDERMAN

Dear New Yorker:

Online research, smartphones, social networks -- technology is a great resource for school and play. However, the world of the web can be as dangerous as the real one and we all need to be cautious. Here are some tips for making use of what the Internet offers without leaving yourself vulnerable.

Stay safe!



Social Networking Sites

While sites like Facebook and Twitter are a great way to keep in touch with friends and family, not all users are well-intentioned. INTERNET PREDATORS and SCAM ARTISTS surf websites in search of their next victim. Simple precautions can ensure that this victim will not be you.

- Adjust your privacy settings to restrict access to friends only.
- Limit the amount of personal information and images you share in your profile (for example, never reveal your address, year of birth or graduation).
- Only "friend" people you know: predators often pose as friends of friends.
- Never agree to meet up with a stranger you "met" online.

Cyber-Bullying

Don't Be a Bully - or Be Bullied

One in four American students has been the victim of cyber-bullying, and at least that many are acting like bullies. Bullying is an assault upon the community, not only the person targeted, and you can play a role in stopping it. If you receive or witness hurtful, embarrassing, or threatening messages:

- Block the sender if the source allows;
- Do not respond to threatening or derogatory messages;
- Tell an adult at school or home that there is a problem and continue to do so until it stops;
- Contact the police if necessary.

Almost all schools have rules in place against cyber-bullying. Many cities and towns either have, or are exploring laws that make cyber-bullying a criminal offense.

Avoid making comments that use teasing or hurtful language. You might think what you're texting or posting is harmless, but it may be hurtful or embarrassing to someone else. Think before you hit the 'send' button, give yourself time to review what you said, or you may end up being labeled a cyber-bully.

Internet Safety Tip Card

Office of the Attorney General
ERIC T. SCHNEIDERMAN

Dear New Yorker:

Online research, smartphones, social networks -- technology is a great resource for school and play. However, the world of the web can be as dangerous as the real one and we all need to be cautious. Here are some tips for making use of what the Internet offers without leaving yourself vulnerable.

Stay safe!



Social Networking Sites

While sites like Facebook and Twitter are a great way to keep in touch with friends and family, not all users are well-intentioned. INTERNET PREDATORS and SCAM ARTISTS surf websites in search of their next victim. Simple precautions can ensure that this victim will not be you.

- Adjust your privacy settings to restrict access to friends only.
- Limit the amount of personal information and images you share in your profile (for example, never reveal your address, year of birth or graduation).
- Only "friend" people you know: predators often pose as friends of friends.
- Never agree to meet up with a stranger you "met" online.

Cyber-Bullying

Don't Be a Bully - or Be Bullied

One in four American students has been the victim of cyber-bullying, and at least that many are acting like bullies. Bullying is an assault upon the community, not only the person targeted, and you can play a role in stopping it. If you receive or witness hurtful, embarrassing, or threatening messages:

- Block the sender if the source allows;
- Do not respond to threatening or derogatory messages;
- Tell an adult at school or home that there is a problem and continue to do so until it stops;
- Contact the police if necessary.

Almost all schools have rules in place against cyber-bullying. Many cities and towns either have, or are exploring laws that make cyber-bullying a criminal offense.

Avoid making comments that use teasing or hurtful language. You might think what you're texting or posting is harmless, but it may be hurtful or embarrassing to someone else. Think before you hit the 'send' button, give yourself time to review what you said, or you may end up being labeled a cyber-bully.

Internet Safety Tip Card

Office of the Attorney General
ERIC T. SCHNEIDERMAN

Dear New Yorker:

Online research, smartphones, social networks -- technology is a great resource for school and play. However, the world of the web can be as dangerous as the real one and we all need to be cautious. Here are some tips for making use of what the Internet offers without leaving yourself vulnerable.

Stay safe!



Social Networking Sites

While sites like Facebook and Twitter are a great way to keep in touch with friends and family, not all users are well-intentioned. INTERNET PREDATORS and SCAM ARTISTS surf websites in search of their next victim. Simple precautions can ensure that this victim will not be you.

- Adjust your privacy settings to restrict access to friends only.
- Limit the amount of personal information and images you share in your profile (for example, never reveal your address, year of birth or graduation).
- Only "friend" people you know: predators often pose as friends of friends.
- Never agree to meet up with a stranger you "met" online.

Cyber-Bullying

Don't Be a Bully - or Be Bullied

One in four American students has been the victim of cyber-bullying, and at least that many are acting like bullies. Bullying is an assault upon the community, not only the person targeted, and you can play a role in stopping it. If you receive or witness hurtful, embarrassing, or threatening messages:

- Block the sender if the source allows;
- Do not respond to threatening or derogatory messages;
- Tell an adult at school or home that there is a problem and continue to do so until it stops;
- Contact the police if necessary.

Almost all schools have rules in place against cyber-bullying. Many cities and towns either have, or are exploring laws that make cyber-bullying a criminal offense.

Avoid making comments that use teasing or hurtful language. You might think what you're texting or posting is harmless, but it may be hurtful or embarrassing to someone else. Think before you hit the 'send' button, give yourself time to review what you said, or you may end up being labeled a cyber-bully.



Do's and Don'ts of Online Purchasing

Purchasing items online is quick and easy, but can leave you open to IDENTITY THEFT and CREDIT CARD SCAMS. Take steps to keep you and your money protected.

- Keep your computer up-to-date on security features like firewalls and anti-virus definitions.
- Make sure the website on which you are considering a purchase is secure. The website's address should start with https:// where the "s" stands for "secure." Look for a "lock" at the bottom right hand corner of your browser window if it's closed, it's secure. Also, check for consumer reviews, privacy policy, a customer service phone number, etc.
- Make sure "discounts" don't involve a monthly fee.
- Print and save all records of the transaction; verify that correct charges are applied to your account.
- Do NOT use wi-fi ports in public places for making online purchases. Such connections are not secure.
- Do NOT use debit cards for Internet purchases. These cards do not carry the fraud protection which credit cards carry.
- Never mail cash or wire money for online purchases.

Downloading Media - If it's free, it might be illegal

Music, movies, games, TV shows...they are all available on the net. It's also illegal to download outside of authorized sources. Downloading "pirated" media, or even sharing files with a friend are serious crimes which are prosecuted, can result in significant jail time and fines in excess of \$150,000. Make sure the media you access online is not pirated, and that you obtain it legally.

Downloading 'free' utilities like screensavers and scanning programs can be dangerous. Many sites offering them are contaminated by malware that can tie up your computer and be very expensive to remove. Avoid these downloads, since even updated antivirus programs may not be effective in preventing the malware from installing itself.

SmartPhones/iPads/etcetera:

These devices are as Internet-connected as a PC. Often, smart-phones do not have enough built-in protection in order to be considered safe for tasks requiring security, such as online banking. Again, look for the "lock," make sure the website is https://. Check to see if your smartphone provides "apps" for security.

Sexting

Sending nude or revealing images of young people over the phone or web is ILLEGAL, regardless of who took the photo. Minors who take and send photographs of themselves can, and have been, charged with producing and distributing child pornography.

These images frequently end up on the internet where anyone can see them, and they stay there forever. This can haunt you for years to come.

NEVER send a sexually revealing image of anyone!



New York State Office
of the Attorney General
www.ag.ny.gov | 1-800-771-7755

Do's and Don'ts of Online Purchasing

Purchasing items online is quick and easy, but can leave you open to IDENTITY THEFT and CREDIT CARD SCAMS. Take steps to keep you and your money protected.

- Keep your computer up-to-date on security features like firewalls and anti-virus definitions.
- Make sure the website on which you are considering a purchase is secure. The website's address should start with https:// where the "s" stands for "secure." Look for a "lock" at the bottom right hand corner of your browser window if it's closed, it's secure. Also, check for consumer reviews, privacy policy, a customer service phone number, etc.
- Make sure "discounts" don't involve a monthly fee.
- Print and save all records of the transaction; verify that correct charges are applied to your account.
- Do NOT use wi-fi ports in public places for making online purchases. Such connections are not secure.
- Do NOT use debit cards for Internet purchases. These cards do not carry the fraud protection which credit cards carry.
- Never mail cash or wire money for online purchases.

Downloading Media - If it's free, it might be illegal

Music, movies, games, TV shows...they are all available on the net. It's also illegal to download outside of authorized sources. Downloading "pirated" media, or even sharing files with a friend are serious crimes which are prosecuted, can result in significant jail time and fines in excess of \$150,000. Make sure the media you access online is not pirated, and that you obtain it legally.

Downloading 'free' utilities like screensavers and scanning programs can be dangerous. Many sites offering them are contaminated by malware that can tie up your computer and be very expensive to remove. Avoid these downloads, since even updated antivirus programs may not be effective in preventing the malware from installing itself.

SmartPhones/iPads/etcetera:

These devices are as Internet-connected as a PC. Often, smart-phones do not have enough built-in protection in order to be considered safe for tasks requiring security, such as online banking. Again, look for the "lock," make sure the website is https://. Check to see if your smartphone provides "apps" for security.

Sexting

Sending nude or revealing images of young people over the phone or web is ILLEGAL, regardless of who took the photo. Minors who take and send photographs of themselves can, and have been, charged with producing and distributing child pornography.

These images frequently end up on the internet where anyone can see them, and they stay there forever. This can haunt you for years to come.

NEVER send a sexually revealing image of anyone!



New York State Office
of the Attorney General
www.ag.ny.gov | 1-800-771-7755

Do's and Don'ts of Online Purchasing

Purchasing items online is quick and easy, but can leave you open to IDENTITY THEFT and CREDIT CARD SCAMS. Take steps to keep you and your money protected.

- Keep your computer up-to-date on security features like firewalls and anti-virus definitions.
- Make sure the website on which you are considering a purchase is secure. The website's address should start with https:// where the "s" stands for "secure." Look for a "lock" at the bottom right hand corner of your browser window if it's closed, it's secure. Also, check for consumer reviews, privacy policy, a customer service phone number, etc.
- Make sure "discounts" don't involve a monthly fee.
- Print and save all records of the transaction; verify that correct charges are applied to your account.
- Do NOT use wi-fi ports in public places for making online purchases. Such connections are not secure.
- Do NOT use debit cards for Internet purchases. These cards do not carry the fraud protection which credit cards carry.
- Never mail cash or wire money for online purchases.

Downloading Media - If it's free, it might be illegal

Music, movies, games, TV shows...they are all available on the net. It's also illegal to download outside of authorized sources. Downloading "pirated" media, or even sharing files with a friend are serious crimes which are prosecuted, can result in significant jail time and fines in excess of \$150,000. Make sure the media you access online is not pirated, and that you obtain it legally.

Downloading 'free' utilities like screensavers and scanning programs can be dangerous. Many sites offering them are contaminated by malware that can tie up your computer and be very expensive to remove. Avoid these downloads, since even updated antivirus programs may not be effective in preventing the malware from installing itself.

SmartPhones/iPads/etcetera:

These devices are as Internet-connected as a PC. Often, smart-phones do not have enough built-in protection in order to be considered safe for tasks requiring security, such as online banking. Again, look for the "lock," make sure the website is https://. Check to see if your smartphone provides "apps" for security.

Sexting

Sending nude or revealing images of young people over the phone or web is ILLEGAL, regardless of who took the photo. Minors who take and send photographs of themselves can, and have been, charged with producing and distributing child pornography.

These images frequently end up on the internet where anyone can see them, and they stay there forever. This can haunt you for years to come.

NEVER send a sexually revealing image of anyone!



New York State Office
of the Attorney General
www.ag.ny.gov | 1-800-771-7755