Promote Online Safety in Your Neighborhood

National Night Out—Cyber Security Checklist

Having a safe community goes beyond safe streets. When you are protected online, you can enjoy the benefits of the digital society.

Protect your personal information

- ○ Use long and strong passwords – the longer it is, the tougher it is to crack. Also use capital and lowercase letters with numbers and symbols to create a more secure password.
- ○ Use a phrase, like "NNOisGreat!" or "Safe2gether"
- ○ Don't share your account passwords with anyone.
- ○ Use different passwords for each account.
- ○ Put your written password reminders in a safe place- not in a file on your computer (that's the first place hackers look).

Keep your computer safe

- ○ Keep your operating system and software updated.
- ○ Be cautious about opening attachments and downloading files from emails, no matter who sent them. Files that look innocent can contain viruses that monitor and control your online activity.
- ○ Make sure your device has anti-virus software and a firewall.
- ○ Never install software from an untrusted source and watch for unwanted add-ons being installed.
- ○ Back up your files: Copy important files onto removable storage (USB flash drive, external hard drive or a cloud service).

Beware of scams

- ○ Watch for email, advertisements, popups, and search results you didn't expect; a scammer may be trying to trick you into sending them money or personal information. This is "Phishing" and criminals use the information to commit identity theft.
- ○ Don't enter sensitive information—Social Security # or credit card—in email, or click links you are unsure about. Legitimate businesses never ask you to send sensitive info via email.

Continued on other side

Promote Online Safety in Your Neighborhood

National Night Out—Cyber Security Checklist

Having a safe community goes beyond safe streets. When you are protected online, you can enjoy the benefits of the digital society.

Protect your personal information

- ○ Use long and strong passwords – the longer it is, the tougher it is to crack. Also use capital and lowercase letters with numbers and symbols to create a more secure password.
- ○ Use a phrase, like "NNOisGreat!" or "Safe2gether"
- ○ Don't share your account passwords with anyone.
- ○ Use different passwords for each account.
- ○ Put your written password reminders in a safe place- not in a file on your computer (that's the first place hackers look).

Keep your computer safe

- ○ Keep your operating system and software updated.
- ○ Be cautious about opening attachments and downloading files from emails, no matter who sent them. Files that look innocent can contain viruses that monitor and control your online activity.
- ○ Make sure your device has anti-virus software and a firewall.
- ○ Never install software from an untrusted source and watch for unwanted add-ons being installed.
- ○ Back up your files: Copy important files onto removable storage (USB flash drive, external hard drive or a cloud service).

Beware of scams

- ○ Watch for email, advertisements, popups, and search results you didn't expect; a scammer may be trying to trick you into sending them money or personal information. This is "Phishing" and criminals use the information to commit identity theft.
- ○ Don't enter sensitive information—Social Security # or credit card—in email, or click links you are unsure about. Legitimate businesses never ask you to send sensitive info via email.

Continued on other side

Promote Online Safety in Your Neighborhood

National Night Out—Cyber Security Checklist

Having a safe community goes beyond safe streets. When you are protected online, you can enjoy the benefits of the digital society.

Protect your personal information

- ○ Use long and strong passwords – the longer it is, the tougher it is to crack. Also use capital and lowercase letters with numbers and symbols to create a more secure password.
- ○ Use a phrase, like "NNOisGreat!" or "Safe2gether"
- ○ Don't share your account passwords with anyone.
- ○ Use different passwords for each account.
- ○ Put your written password reminders in a safe place- not in a file on your computer (that's the first place hackers look).

Keep your computer safe

- ○ Keep your operating system and software updated.
- ○ Be cautious about opening attachments and downloading files from emails, no matter who sent them. Files that look innocent can contain viruses that monitor and control your online activity.
- ○ Make sure your device has anti-virus software and a firewall.
- ○ Never install software from an untrusted source and watch for unwanted add-ons being installed.
- ○ Back up your files: Copy important files onto removable storage (USB flash drive, external hard drive or a cloud service).

Beware of scams

- ○ Watch for email, advertisements, popups, and search results you didn't expect; a scammer may be trying to trick you into sending them money or personal information. This is "Phishing" and criminals use the information to commit identity theft.
- ○ Don't enter sensitive information—Social Security # or credit card—in email, or click links you are unsure about. Legitimate businesses never ask you to send sensitive info via email.

Continued on other side

Connect with care

- Use web addresses with “https://” for all sites you log into or for online purchasing. The “**s**” stands for “secure” and the site encrypts your information.
- Secure your home wireless network with a strong password and WPA2 encryption.
- Use your browser’s privacy and security settings, such as pop-up blockers.
- Watch your links:
  - If you have a question about a link on a website, put your mouse over it *without* clicking. Your browser will show you the actual address of the destination web page. If everything looks okay, you can then click. If not, STOP!
  - Is it the official site? Example:
    - service@paypal.com = good
    - service@paypal.com.clickz.com = bad

Talk with your kids

- Make sure your kids know not to share passwords and personal information. Make sure they understand the dangers of scams or malware advertised as "free” downloads of music, movies, iPads, and software or games. If it looks too good to be true, it probably is!
- Look for teachable moments — if you hear about a scam, phishing message or cyberbullying, use it as an example with your kids.
- Know which social networking sites they use and “friend” them so you can monitor their use.

Help your community

- Share cyber safety tips with your friends, family and neighbors.
- File cybercrime reports with the Minneapolis Police Department, with www.ic3.gov or the Federal Trade Commission www.ftccomplaintassistant.gov

More Resources

- Explore resources at www.consumer.ftc.gov for privacy, identity and online security tips.
- Check out www.cisa.gov/publication/stop-think-connect-toolkit to use toolkits for families, educators and more.

Connect with care

- Use web addresses with “https://” for all sites you log into or for online purchasing. The “**s**” stands for “secure” and the site encrypts your information.
- Secure your home wireless network with a strong password and WPA2 encryption.
- Use your browser’s privacy and security settings, such as pop-up blockers.
- Watch your links:
  - If you have a question about a link on a website, put your mouse over it *without* clicking. Your browser will show you the actual address of the destination web page. If everything looks okay, you can then click. If not, STOP!
  - Is it the official site? Example:
    - service@paypal.com = good
    - service@paypal.com.clickz.com = bad

Talk with your kids

- Make sure your kids know not to share passwords and personal information. Make sure they understand the dangers of scams or malware advertised as "free” downloads of music, movies, iPads, and software or games. If it looks too good to be true, it probably is!
- Look for teachable moments — if you hear about a scam, phishing message or cyberbullying, use it as an example with your kids.
- Know which social networking sites they use and “friend” them so you can monitor their use.

Help your community

- Share cyber safety tips with your friends, family and neighbors.
- File cybercrime reports with the Minneapolis Police Department, with www.ic3.gov or the Federal Trade Commission www.ftccomplaintassistant.gov

More Resources

- Explore resources at www.consumer.ftc.gov for privacy, identity and online security tips.
- Check out www.cisa.gov/publication/stop-think-connect-toolkit to use toolkits for families, educators and more.

City of Minneapolis Information Technology Department
July 2021 www.minneapolismn.gov/it/inclusion
Minneapolis City of Lakes

Connect with care

- Use web addresses with “https://” for all sites you log into or for online purchasing. The “**s**” stands for “secure” and the site encrypts your information.
- Secure your home wireless network with a strong password and WPA2 encryption.
- Use your browser’s privacy and security settings, such as pop-up blockers.
- Watch your links:
  - If you have a question about a link on a website, put your mouse over it *without* clicking. Your browser will show you the actual address of the destination web page. If everything looks okay, you can then click. If not, STOP!
  - Is it the official site? Example:
    - service@paypal.com = good
    - service@paypal.com.clickz.com = bad

Talk with your kids

- Make sure your kids know not to share passwords and personal information. Make sure they understand the dangers of scams or malware advertised as "free” downloads of music, movies, iPads, and software or games. If it looks too good to be true, it probably is!
- Look for teachable moments — if you hear about a scam, phishing message or cyberbullying, use it as an example with your kids.
- Know which social networking sites they use and “friend” them so you can monitor their use.

Help your community

- Share cyber safety tips with your friends, family and neighbors.
- File cybercrime reports with the Minneapolis Police Department, with www.ic3.gov or the Federal Trade Commission www.ftccomplaintassistant.gov

More Resources

- Explore resources at www.consumer.ftc.gov for privacy, identity and online security tips.
- Check out www.cisa.gov/publication/stop-think-connect-toolkit to use toolkits for families, educators and more.

City of Minneapolis Information Technology Department
July 2021 www.minneapolismn.gov/it/inclusion
Minneapolis City of Lakes