Keeping your Family Safe Online:
Securing your Home and Devices

Lisa Plaggemier
Interim Executive Director,
National Cyber Security Alliance

Frances Dewing
Head of Product for Consumer & Small Business, Palo Alto Networks

Kelli Andrews
Senior Director of Cybersecurity and Lawful Access, Microsoft

Carlos Sotero
Chief Information Officer,
Allstate Identity Protection
Why you should care: Reason #1

Leader

- Virus writer/Programmer
- Malware-packing service
- System administrator
- Assistant
- Traffic dealer
- Spammer
- Downloads
- Distributors
- Head of the money mules service
- Money mules manager
- Money mules
- Cash withdrawal
- Money flow manager
Why you should care: Reason #1 (cont’d)

- Malware tools
- Phishing kits
- Step by step instructions on how to set up an attack
- Customer technical support
- Money back guarantees
- Data on who to target
Why you should care: Reason #2
Common threats & real examples
Phishing
The impersonator, fraudster, smooth-talker, bait and switch

Rap Sheet
- Convincing impersonator (of brands you trust & people you know)
- Tries get you to take an action — click, view, download, respond — and give up personal info, or download something (aka, malware)
- Not just email; can come through SMS, social, apps, etc.
- Preys on social/global trends & sense of urgency

Recent Impersonations
- Security alert related to your Apple account login
- Problem with your paycheck/payroll deposit
- Amazon shipment requires your action
- LinkedIn recruiter; view this job
Malware
The spy, the infiltrator, the pickpocket, the bomb planter

Rap Sheet
• Variety of skills includes: spying and exfiltrating data for next-stage attacks, ransoming, capturing keystrokes, stealing credentials
• Can come in the form of websites, links, images, ads, and files.
• Often works together with Phishing

Recent Impersonations
• “Sharon invited you to view a document” (Google Doc, attachment)
• “Install this free game/free skin” (Ad pop-up in mobile game)
IoT Vulnerabilities
The opportunist, the lock-jiggler

Rap Sheet
- Takes advantage of security weaknesses in IoT devices
- Targets latent vulnerabilities in devices that aren't built with security in mind
- Uses IoT device as an entry point into other devices on the home network

Recent Impersonations
- Taking advantage of default username/password to access security cameras and steal copies of video
- Intercepting baby monitor feeds
- Home control heating/lighting systems
- Smart locks on doors
3 ways to stay safe
Protect your accounts

**Top tip:**
Turn-on multi-factor authentication

- Something you know & something you have
- Turn it on everywhere - esp. Emails, social media, financial account logins, apple iCloud (file sync/device data sync)

**Pro tip:**
App-generated is better than text is better than email
Protect your devices

Top tip:
Keep software updated & turn on (free) built-in security

- Almost all software updates include a security patch for known vulnerabilities
- Update operating system as well as any apps or software installed
- For computers: Turn on OS firewall

Pro tip:
Make backups of your data
Protect your network

Top tip:
Use a network firewall with advanced threat blocking

- Antivirus is not enough. Stop threats before they reach your devices
- Some business-grade routers have this capability, but security effectiveness varies
Thanks for tuning in.
Stay safe online.

Website
StaySafeOnline.org

Twitter
@staysafeonline

Facebook
/staysafeonline

LinkedIn
/national-cyber-security-alliance

Email
info@staysafeonline.org
3 ways to stay safe

**Protect your accounts**

**Top tip:** Turn-on multi-factor authentication

- Something you know & something you have
- Turn it on everywhere — esp. Emails, social media, financial account logins, apple iCloud (file sync/device data sync)

**Pro tip:** App-generated is better than text is better than email

**Protect your devices**

**Top tip:** Keep software updated & turn on (free) built-in security

- Almost all software updates include a security patch for known vulnerabilities
- Update operating system as well as any apps or software installed
- For computers: Turn on OS firewall

**Pro tip:** Make back-ups of your data

**Protect your network**

**Top tip:** Use a network firewall with advanced threat blocking

- Antivirus is not enough. Stop threats before they reach your devices
- Some business-grade routers have this capability, but security effectiveness varies

**Pro tip:** Okyo does this for you; it protects your network and all connected devices on it