National Institutes of Health

Cyber Safety. Protect our People and our Science.

I let him use my work laptop to play a game,
But when I logged back in, something was off.

Julie's Cyber Safety Story – "I Let My Son Use My Laptop."

Each month the Cyber Safety Awareness Campaign team will be sharing a story that's based on a real-life cybersecurity risk or incident at NIH. This effort is meant to raise awareness that cyber safety is a very real concern for all of us at NIH.

"My name is Julie, and this is the story of what happened when I let my ten-year-old son use my NIH laptop."

I had wrapped up working from home and was starting to make dinner when my son walked in. He wanted to know if he could use my NIH laptop to play a game he had heard about online.

Hoping to keep him busy until dinner was ready, I logged into the computer for him and left to finish cooking.

Later that evening, I opened my laptop to check my email and immediately noticed a pop-up message saying that my system had been compromised by malware. That's when it hit me that I had made a huge mistake. I called the NIH IT Service Desk to report a cyber incident.

Which of the following remote work best practices could have helped Julie prevent this potentially dangerous cybersecurity incident?

A. Never allow anyone, even your family, to use your government-issued equipment
B. Only allow others to use your government-issued equipment with close supervision
C. Use a designated space within your home as a remote work office to control access

To find out the correct answer(s) and learn more about working from home securely, visit the Sharing Our Cyber Stories page on the Cyber Safety Awareness Campaign website.

Thank you for your ongoing commitment to cyber safety. Your hard work enables us to continue to Protect our People and our Science and to safeguard the mission of the NIH.

Best,

Jothi Dugar
Cyber Safety Awareness Campaign Lead

Information Security

Return to: NIH OCIO > IT Governance & Policy

Cyber Safety Awareness Campaign – Sharing Our Cyber Stories

OUR CYBER STORIES

You asked, we listened. We know that making cyber risks real makes it easier for all of us to prioritize cyber safety in our daily work. That's why, over the past few months, we've been collecting stories across NIH about real-life cybersecurity incidents and risks. Each month, we'll be sharing a new story inspired by a real-life risk or incident to help us all learn and grow as a cyber-safe community.

Click to Read | Remote Work | Sensitive Information

Julie's Cyber Safety Story – "I Let My Son Use My Laptop"

"My name is Julie, and this is the story of what happened when I let my ten-year-old son use my NIH laptop."

I had wrapped up working from home and was starting to make dinner when my son walked into the kitchen.

He asked if he could use my NIH laptop to play a game he had heard about online. Hoping to keep him busy until dinner was ready, I logged into the computer for him and left to finish cooking.

Later that evening, I opened my laptop to check my email and immediately noticed a pop-up message saying that my system had been compromised by malware. That's when it hit me that I had made a huge mistake. I called the NIH IT Service Desk to report a cyber incident.

Which of the following remote work best practices could have helped Julie prevent this potentially dangerous cybersecurity incident?

A. Never allow anyone, even your family, to use your government-issued equipment

B. Only allow others to use your government-issued equipment with close supervision

C. Use a designated space within your home as a remote work office to control access

✓ Answer

There are a few things that Julie could have done to prevent this incident from happening:

A. Never allow anyone, even your family, to use your government-issued equipment

C. Use a designated space within your home as a remote work office to control access

When you are working from home it's more important than ever to remember that your government-issued equipment is for your use only. It is against NIH policy to allow anyone else to use your log-in information for any reason, including family and friends.

To assist with keeping work files and equipment safe, NIH recommends that you designate a space within your home for remote work, such as an office or bedroom. Keeping your work equipment and files in a closed room may help children understand that these items are tools for you to use, not toys for them to play with.

Want to Learn More?

Check out this quick resource on how to work securely from home.

Have your own cybersecurity story? Share it here.

Click the button below to share your own real-life cyber safety story. Your experiences will help others across NIH understand the reality of cyber risk.

SHARE MY STORY

Click here for instructions on how to use the challenge's crowdsourcing website.

Cyber Safety Resources

- **Resources for Children and Families**
- **Cyber Safety & COVID-19**
- **Leadership Toolkit**
- **Cyber Safety Tips & Tricks**
  - Phishing
  - Physical & Logical Security
  - Travel
  - Remote Work
  - Protecting Sensitive Information
- **OCIO Security Awareness Gallery**
- **Department of Homeland Security – National Cybersecurity Awareness Month Resources**
- **Find Your Information System Security Officer (ISSO)**
- **Find Your Privacy Coordinator**

Campaign Sponsors

Andrea Norris
Chief Information Officer

Patrick Shirdon
Director of Management
National Institute on Aging

Stacie Alboum
Deputy Director
Center for Info. Tech.

Campaign Lead

Jothi Dugar
Chief Information Security Officer
Center for Information Technology