THE Heartland CLUB

N ♥ E ♥ W ♥ S ♥ L ♥ E ♥ T ♥ T ♥ E ♥ R

SEPTEMBER 2018

Our 2018 Christmas show is - *Holly Jolly Christmas – A Holiday Revue - Sunday, December 2nd*
THE PALACE THEATER IN THE DELLS, WISCONSIN DELLS
The Palace continues its seasonal tradition of presenting an all-new Holiday Revue for the entire family. This heart-warming show is packed full of classic and contemporary song and dance featuring incredible performers, stunning costumes and dazzling sets. Our spectacular holiday celebration is sure to re-kindle the true Christmas spirit in all of us. Don't miss this festive favorite for the entire family!
Don't wait make your reservations NOW to join us on this upcoming trip - BROCHURE ENCLOSED.

Contact Deb Poad at 608-987-3321 with any questions you may have. Pat and I look forward to seeing you on our upcoming trip.

Deb Poad – Pat Forbes, Club Coordinators

STOPPING SCAMS TARGETING OLDER CONSUMERS
The Federal Trade Commission (FTC) has a long history of protecting people from scams. As part of its ongoing efforts to protect people in every community, the FTC recently took steps to stop schemes harming older adults.
The latest tech support scam, which appears to impact older adults, has a lot in common with other scams we've seen. Some scammers pretend to be calling from the technical support department of a well-known company. Others send pop-up messages warning you about a problem with your computer. They want you to believe your computer is infected with a virus, or that a hacker is trying to access your computer. It's all a ploy to get you to pay for bogus technical support you don't need.
HOW THE SCAM WORKS
Scammers may call, place alarming pop-up messages on your computer, offer free "security" scans, or set up fake websites, all to convince you that your computer is infected. The scammers try to get you on the phone, and then work to convince you there's a problem. Finally, they ask you to pay them to fix that non-existent problem.
To convince you that both the scammers and the problems are real, the scammers may:

- Pretend to be from a well-known company – like Microsoft or Apple
- Use lots of technical terms
- Ask you to get on your computer and open some files – and then tell you those files show a problem (when they don't)

CONTINUE NEXT PAGE

Then, once they've convinced you that your computer has a problem, the scammers might:

- Ask you to give them remote access to your computer – which lets them change your computer settings to your computer is vulnerable to attack
- Trick you into installing malware that gives them access to your computer and sensitive data, like user names and passwords
- Try to sell you software that's worthless, or that you could get elsewhere for free
- Try to enroll you in a worthless computer maintenance or warranty program
- Ask for credit card information so they can bill you for phony services, or services you could get elsewhere for free
- Direct you to websites and ask you to enter your credit card number and other personal information

These scammers want to get your money, access to your computer, or both. But there are things you can do to stop them.

IF YOU GET A CALL OR POP-UP

- If you get an unexpected or urgent call from someone who claims to be tech support, hang up. It's not a real call. And don't rely on caller ID to prove who a caller is. Criminals can make caller ID seem like they're calling from a legitimate company or a local number
- If you get a pop-up message that tells you to call tech support, ignore it. There are legitimate pop-ups from your security software to do things like update your operating system. But do not call a number that pops up on your screen in a warning about a computer problem.
- If you're concerned about your computer, call your security software company directly – but don't use the phone number in the pop-up or on caller ID. Instead, look for the company's contact information online, or on a software package or your receipt.
- Never share passwords or give control of your computer to anyone who contacts you.

IF YOU WERE SCAMMED

- Get rid of malware. Update or download legitimate security software and scan your computer. Delete anything the software says is a problem.
- Change any passwords that you shared with someone. Change the passwords on every account that uses passwords you shared.
- If you paid for bogus services with a credit card, call your credit card company and ask to reverse the charges. Check your statements for any charges you didn't make and ask to reverse those, too. Report it to ftc.gov/complaint.

REFUND SCAMS

If you paid for tech support services, and you later get a call about a refund, that call is probably also a scam. Don't give the person any personal or financial information.

The refund scam works like this: Several months after a purchase, someone calls to ask if you were happy with the service. If you say "No", the scammer offers a refund. Or, the caller says the company is going out of business and giving refunds. The scammer eventually asks for your bank or credit card account number, or asks for access to your bank account to make a deposit. But instead of putting money in your account, the scammer takes money from your account.

If you get a call like this, hang up, and report it: ftc.gov/complaint.

PLEASE REPORT SCAMS

If you spot a scam, please report it to the Federal Trade Commission. Report scams online or call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261. Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the scammers and stop them before they can get someone's hard-earned money. ***It really makes a difference.***

https://www.consumer.ftc.gov/blog/2018/02/stopping-scams-targeting-older-consumers

** Information reprinted from Iowa County News & Views – May 2018 issue

By: Alvaro Puig, Consumer Education Specialist, FTC