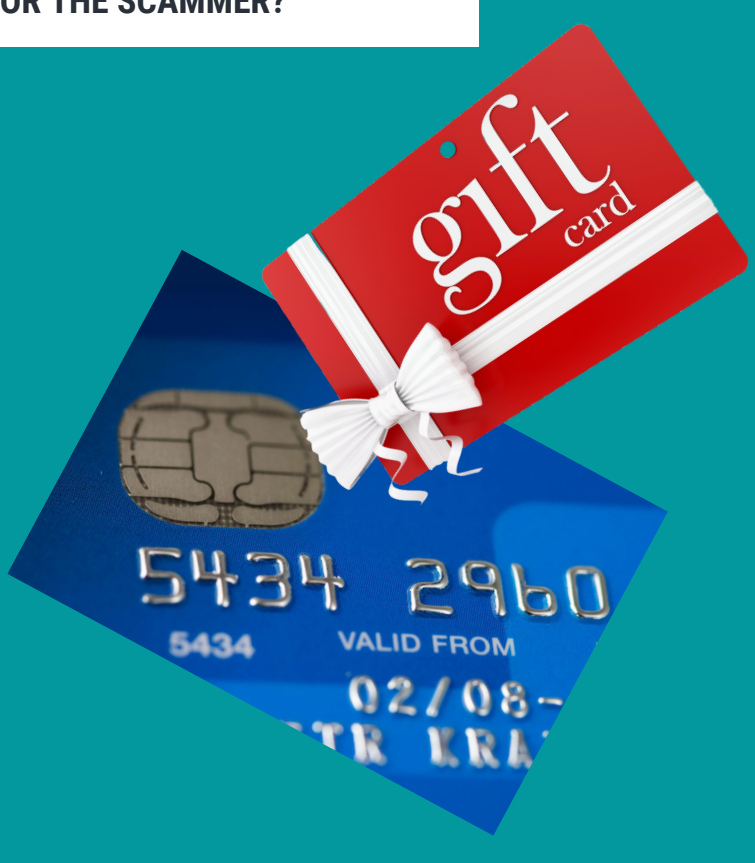
DON'T GET CAUGHT IN A TECH SUPPORT SCAM!

HOW DO TECH SUPPORT SCAMS WORK?

Tech support scammers may call you, enlist pop-up ads on your computer, or place ads for their "tech support company" to look credible and attempt a scam. They often gain control of your computer by asking you to give them remote access to your computer. Once they gain access, the scammer may pretend to run a diagnostic test of your computer. In reality, they are downloading malware, or other viruses, downloading sensitive information that was stored on your computer, or locking you out of your computer by downloading ransomware.

WHAT'S IN IT FOR THE SCAMMER?

- **Obtain sensitive information**
- **Find credit card information**
- **Ask you to pay to fix an issue that doesn't exist with a wire transfer, gift card, or credit card. Though some will ask you for credit card information, the scammer often asks you to pay by wiring money, putting money on a gift card, prepaid card or cash reload card, or using a money transfer app because they know those types of payments can be hard to reverse.**



SPOTTING AND AVOIDING TECH SUPPORT SCAMS

Tech support scammers use many different tactics to trick people. Spotting these tactics will help you avoid falling for the scam.

Phone Calls (Vishing)

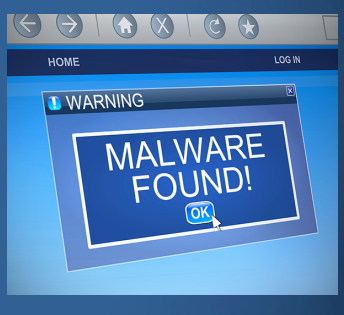
Tech support scammers may call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist.
If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up and notify your IT department.

Emails (Phishing)

Phishing = The use of malicious emails that cause the recipients to divulge sensitive information or perform a task to bypass the computer's security. It can often be difficult to determine whether an email is legitimate or a phishing email - but there are signs to look for. Review the email address from which it was sent. the name it was sent to, and check if this is the phone number you have been instructed to use to contact your IT dept.

Text Messages (Smishing)

An SMS message will instruct the recipient to contact a customer support line via a number that's provided. Once on the line, the scammer will try to gather information from the caller by pretending to be a legitimate technical service representative.
If you get a text message stating there's a problem with your computer, immediately notify your IT department.



Pop-up Warnings

Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.

Online Ads and Listings in Search Results Pages

Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online. The scammers are hoping you'll call the phone number to get help.
If you are in need of assistance, contact your IT department.

I WAS SCAMMED! WHAT DO I DO NOW?

- **If you gave your user name and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.**
- **If you believe you have fallen victim to a tech support scam contact your IT department immediately.**

DON'T HESITATE TO CHECK THESE RESOURCES FOR MORE INFORMATION

For more information regarding work use of home computers, visit these sites:

- Oneida Co. Acceptable Use Policy
- NYS Information Security Policy
- NYS Acceptable Use of Technology Resources Policy

Don't hesitate to contact the IT department if you need assistance with determining if an email is a scam.

Better to be safe than sorry!

ONEIDA COUNTY
www.ocgov.net