Willow Valley Computer Club

Programs are at 2:00 pm the first Thursday of the month (except July-August) in the Cultural Center unless otherwise noted.

Inside this issue:

- Human Hacking

- Volunteer Needed

Computer Club Leadership

- President: Al Williams
- Vice President: Dick Beidleman
- Secretary: Paula Sandridge
- Treasurer: Lee Wermuth
- Previous President: Sid Paskowitz

Committee Chairpersons

- Apple SIG:
- Club Website: Paula Sandridge
- Computer Room: Lee Wermuth
- Information Central: Sid Paskowitz
- Newsletter: Mike Pancione
- Program: Dick Beidleman & Bob Schaffer
- Publicity: Bill Adams
- SmartLife: Al Fulvio
- Training: Bill Skelly
-

Director

- CCTC: Cathy Thorn

Advisors

- Bruce Mawson
- Tony Poulos
- Bob Scala
- John Santora

President's Pen *by Al Williams*

Welcome to the Computer Club's July Newsletter!

We're taking a break from monthly presentations for the summer, but we'll restart them in September. We're not taking a break from our educational programs, most of which are described in the Renaissance and listed on our website, wvcomputerclub.org, under Calendar. We anticipate having a couple of surprise educational programs this summer. We'll announce them later.

How do hackers influence and manipulate the people they're hacking? You should know how it's done and that you're not alone if you are scammed. Some have lost thousands of dollars. Learn more in this issue.

Do you have a question or want to provide feedback? Please get in touch with us at wvcomputerclub@gmail.com.

"I don't know why I did what I did."

"I don't understand why."

"I feel so stupid."

When I ask residents who've been scammed why they responded to the scammers, they typically give me responses like those above. You may think these people are stupid if you've never been scammed. But the truth is, anyone can be scammed. It's not about intelligence; it's about context, emotional triggers, psychological principles, and the application of social engineering. The fact is, we're all susceptible to these tactics. Although scamming humans was an art, it's now mostly science. Becoming familiar with these factors can help minimize the likelihood of falling victim to a scam.

In his book *Social Engineering: The Science of Human Hacking, 2nd Edition,* professional social engineer Christopher Hadnagy describes how he conducts face-to-face and media-based human hacking on behalf of clients who want to know if their company is vulnerable to hackers. The methods in his book are not just theories but are based on extensive research. This research explains how scams are successful, providing a wealth of knowledge for those who want to protect themselves.

The hacker aims to get you, the target, to make decisions based on emotions rather than rational thinking.

The hacker begins by framing a scam, which considers the context and a message containing triggers that will cause the target to respond. I'll explain how this is done for these scams:
- Tech support with scareware
- Phishing
- Romance

Tech support with scareware scam
The *tech support with scareware scam* relies on several factors: (This is the scam in which the target's computer screen displays a message that the computer has been infected and a voice commands the target to call a number and not to turn the computer off.)
- The target knows that something can go wrong with a computer.
- The target is relaxed and likely daydreaming; the target's mind is in alpha mode.
- The tech support scareware message suddenly appears on the computer screen. The scam uses Microsoft's name as the authority that is declaring the target's computer infected. A voice commands the target to call the number on the screen and not turn off the computer.
- With fear, the target calls the number on the screen, contacting the scammer. The scammer then works with the target to help resolve the problem. The scammer directs the target to download remote access software (allegedly to get rid of the malware).
- As the scammer supposedly helps the target, the scammer uses the Principle of Reciprocity (where we feel we have to pay back the one giving help) to get the target to help him.
- At some point, the target realizes they are being scammed, stops working with the scammer, and asks for help.

(continued)

When you realize you are being scammed, you should promptly turn off your computer. You are not alone; others have been through this; there is help. You should notify your bank and the credit bureaus. You should file a report with local law enforcement (West Lampeter Township Police). You should go to usa.gov/where-report-scams to find the proper federal agency to report the scam. You should file a report with Willow Valley by filing an online Service Request. The Computer Club can help you secure your computer. Contact us at <u>wvcomputerclub@gmail.com</u>.

Phishing scam

Another scam is *phishing*. In this scam, the scammer sends a false email that appears to come from a well-known (authoritative) source such as CVS, Kohls, or PayPal. Phishing emails are becoming harder to recognize as scammers purchase realistic phishing templates or use AI to help them create highly plausible emails. The scammer's goal may be to get the target to respond to the attractive offer by clicking on a link to claim the offer.

One of two possible scenarios may occur if the target clicks on the link. The scammer will direct the link to a website that looks like CVS, Kohls, or PayPal. The target enters their username and password, which the scammer captures and uses on the actual website.

Or, the scammer's link may download malware onto the target's computer, thereby establishing a beachhead for the scammer to access the target's computer at will without the target's knowledge. The scammer may capture usernames, passwords, credit card numbers, and more.

A preferred way to determine if it is a phishing email is to call the organization directly. It is essential to go to the organization's website and find their phone number. Residents have googled for phone numbers, such as googling for PayPal Customer Service, only to go to a scammer's website offering the service. At that point, the target finds themselves in the *tech support with scareware* scam.

Romance scam

The *romance scam* is especially devastating because of the money lost and the emotional distress. Typically, a woman approaches a man on social media, such as Facebook. However, a man could approach a woman. In either case, a friendship develops, and the scammer eventually tells the target they trust them.

The statement causes oxytocin and dopamine to be released into the target's bloodstream, causing the target to associate a feeling of trust with the scammer. This trust can make the target do something they instinctively know is not in their best interests. For example, scammers have successfully asked targets to pay their medical bills, apartment rent, and other expenses. Other scammers have deceived targets into investing in crypto, but the crypto investment invariably fails, and all money is lost.

Romance scammers continue to ask for money from the target until either the target loses all their money or realizes what is happening and stops the scam.

If you are involved in a romance scam, you are not alone. Others have been through this, and there is help. You should notify your bank and the credit bureaus. You should file a report with local law enforcement (West Lampeter Township Police). Then, you should go to usa.gov/where-report-scams to find the proper federal agency to report the scam. You should file a report with Willow Valley by filing an online Service Request. The Computer Club can help you secure your computer. Contact us at wvcomputerclub@gmail.com.

Residents have lost thousands of dollars to these scams!

Summary

These are the most frequent scams, but there are many others, such as online shopping and investment scams. The Federal Trade Commission reports that more than $10 billion was lost to scams in 2023, an increase of 14% from 2022. 2.6 million consumers submitted fraud reports in 2023, nearly the same as in 2022.

We're all susceptible to scams. When you receive unexpected emails or unexpected attempts to contact you, be suspicious. Being aware of how scammers conduct scams and being skeptical will help us avoid scams.

Beyond this overview of scams tutorial, the Willow Valley Computer Club provides training and presentations with additional information about many topics, including protecting yourself from scams, the data on your computer, and your personal identifying information.

Note: Jay Shah and Bill Skelly reviewed this tutorial.

WVCC mission: "to provide the means to educate beginners or interested non-users on how to use a computer"

WVCC mission: "to provide a forum for interchange of computer information among members"

WVCC mission: "to arrange for speakers to talk about subjects of interest to those with some background and experience in computer use"

Contact Information

For more information about the Computer Club, please contact Al Williams via email at wvcomputerclub@gmail.com.

Please keep your email address on Club records current so we can send you important emails. Send email corrections or updates to Lee Wermuth at lwermuth582@gmail.com.

Bill Skelly is the Willow Valley Computer Club Training Coordinator. We are always looking for residents qualified to teach computer-related topics. We want our classes to support your needs. Contact Bill (whskelly@aol.com) to volunteer or to offer ideas on topics needed.

Computer Club Technology Center

NOTE: The Computer Club Technology Center (CCTC) is open on Mondays only, from 10 am to 4 pm. The CCTC is located on the 5th floor of Manor North 'J 'building. The door may be closed, but with a sign indicating *Please Knock.*

Apple Items Available: See Bruce Thompson in the CCTC.

Willow Valley Computer Club
Volunteer Opportunity

Volunteer Position Title: Deputy CCTC Director

Description of Role: Assists the CCTC Director as needed to accomplish the objectives set forth by the Willow Valley Computer Clubs's Executive Committee

Training: The CCTC Director will provide training as needed for the Deputy CCTC Director to accomplish their assignments

Reporting: The Deputy CCTC Director will report to the CCTC Director
Time Commitment: A minimum of 4 hours per week is needed. The candidate must be able to work during the hours acceptable to the CCTC Director

Qualifications: Prior operations experience is desirable. A willingness to learn is imperative