# SECURITY ADVISORY

Willow Valley Computer Club

## Fake Evite Emails: How They Work and How to Protect Yourself

June 2026

## What Is Happening?

Residents at Willow Valley have been receiving fraudulent electronic invitations (**"evites"**) that appear to come from friends and neighbors. These are not harmless spam. They are the visible part of a **credential-harvesting attack**—a method attackers use to steal your email password, take over your account, and then use your identity to attack everyone in your contact list.

This advisory explains exactly how the attack works from a technical standpoint, why it is particularly dangerous, and what to do if you have already interacted with one of these messages.

## How the Attack Works, Step by Step

Understanding each stage of this attack is important because it reveals where the real danger lies—and it is **not** in the evite itself.

### Stage 1: The Bait

You receive an email that looks like a legitimate party invitation, holiday gathering, or community event. It may appear to come from someone you know—a neighbor, a fellow resident, or a family member. The email contains a button or link that says something like "View Your Invitation" or "RSVP Now."

At this point, nothing harmful has happened. **Simply receiving or even opening the email does not compromise your account.** The danger begins with the next step.

### Stage 2: The Trap

When you click the link, you are taken to a website that **looks like** a sign-in page for Gmail, Yahoo, Outlook, or whatever email provider you use. The page may be a near-perfect visual copy of the real thing. It asks you to enter your email address and password to "view your invitation."

**This Is the Critical Moment**

A real invitation service like Evite shows you the invitation immediately. It **never** asks for your email password. Any page that asks for your email credentials after clicking an invitation link is the attack—no exceptions.

### Stage 3: The Takeover

If you enter your email password on that page, the attacker now has it. Within minutes—often within seconds, using automated software—the attacker does the following:

1. **Signs in to your email account** using the password you just provided. From the attacker's perspective, this is not "hacking"—you gave them the correct credentials, so the email provider lets them right in.
2. **Downloads your entire contact list**—every email address of every person you have ever corresponded with. This includes family members, neighbors, doctors' offices, financial advisors, club members, and anyone else in your address book.
3. **Sends a new round of fake evites** to every person in your contacts. Because these messages come from (or appear to come from) **your** email address, the recipients are far more likely to trust and click on them. This is what makes the attack self-propagating—each victim produces the next wave.
4. **Scans your inbox and sent mail** for valuable information. This is where the consequences extend far beyond email.

## Why This Is More Dangerous Than It Appears

Many people think the worst consequence of a compromised email is that "some spam gets sent in my name." That is dramatically understating the risk. Your email account is the **master key** to your entire digital life. Here is why:

### Password Resets for Banking and Financial Services

When you click "Forgot Password" on your bank's website, where does the reset link go? **Your email.** An attacker who controls your email account can request password resets for your bank, your credit card company, your investment accounts, and your retirement fund. They receive the reset link, set a new password, and lock you out of your own financial accounts.

### Online Shopping and Retail Accounts

Accounts at Amazon, Walmart, and other retailers typically have a credit card or bank account already on file. An attacker can reset those passwords through your

compromised email, sign in, and make purchases using your stored payment methods—all before you realize what has happened.

### Insurance, Medical, and Government Portals

Many residents access Medicare, Social Security, insurance portals, and patient health records through accounts that use email-based password recovery. A compromised email address can provide a pathway into these systems, exposing sensitive personal and medical information.

### Your Email Archive Is a Treasure Trove

Even without resetting any passwords, your inbox and sent folder likely contain years of correspondence that include account numbers, partial Social Security numbers, tax documents, insurance policy numbers, medical information, and personal details that can be used for identity theft.

## Why Evite-Style Attacks Are So Effective

Attackers have chosen the evite format deliberately. It exploits several psychological patterns:

- **Social trust.** The invitation appears to come from someone you know. You're not evaluating a message from a stranger—you're responding to a friend.
- **Implied urgency.** "RSVP by Friday" or "You're invited!" creates a gentle pressure to act quickly without stopping to think.
- **Single-click simplicity.** There is no suspicious attachment to download. The action is just clicking a link—something we do dozens of times a day.
- **The credential page looks familiar.** The fake sign-in page only needs to look right for a few seconds. Most people don't examine URLs carefully before typing a password.

## How to Protect Yourself

### The Golden Rule

If you click on any link—in an evite, an email, or a text message—and the resulting page asks you to enter your **email password**, **STOP.** Close the page. That is the attack.

Beyond that golden rule, here are additional protective steps:

- **Verify before you click.** If you receive an evite from someone you know, contact them by phone or in person to ask if they actually sent it. Do not reply to the email—the attacker may be reading it.
- **Look at the web address (URL).** Before entering any password, check the address bar in your browser. A legitimate Gmail sign-in page will show "accounts.google.com." A fake one will show something different—often a long or unusual web address.
- **Use different passwords for different accounts.** If your email password is also your bank password, a single compromise exposes everything. A password manager such as Bitwarden can help you maintain unique passwords without having to memorize them all.
- **Enable two-factor authentication (2FA).** This adds a second step to signing in—typically a code sent to your phone. Even if an attacker steals your password, they cannot get in without that second code. Most major email providers offer this for free.

## What to Do If You Already Clicked and Entered Your Password

If you have already entered your email credentials on a suspicious page, take these steps **immediately.** Every hour of delay gives the attacker more time to use your account.

1. **Change your email password right now.** Go directly to your email provider's website by typing the address yourself (do not click any links from emails). Change your password to something completely new. The hacker may change your password and lock you out.
2. **Enable two-factor authentication.** While you are in your account settings changing your password, turn on two-factor authentication. This prevents the attacker from getting back in even if they had your old password.
3. **Check your sent folder and account activity.** Look for emails you did not send. Most email providers also have a "Recent Activity" or "Security" page that shows recent sign-ins, including the location and device. If you see unfamiliar sign-ins, the attacker was in your account.
4. **Change passwords on financial and retail accounts.** Any account that uses your email address for password recovery should be considered at risk. Prioritize

banking, credit cards, investment accounts, and major retail accounts (Amazon, etc.).

5. **Notify your contacts.** Let friends and family know that fake messages may have been sent from your address. A simple phone call or text message is sufficient: “If you received an evite from me, don’t click on it—my email was compromised.”
6. **Contact the WVCC Help Desk.** If you need assistance with any of these steps, send an email to gethelp@wvcomputerclub.org, visit the CCTC on Thursdays between 10:00 AM and 4:00 PM, or call us at 717-464-6330. Our volunteers can walk you through securing your accounts.

---

You’ve always been valuable, but now you’re **visible and reachable.** Understanding how these attacks work is your best defense. The attacker isn’t relying on technical sophistication—they’re relying on trust and speed. A moment of caution when you see a password prompt is all it takes to stop the chain.

If you have questions or concerns, please reach out to the WVCC Help Desk at **gethelp@wvcomputerclub.org.**

*Al Williams*
*For the Executive Committee*
*Willow Valley Computer Club*