

SAVCC

Is it a

SCAM!



Tuesday, April 16th
9:30 - 11:30 a.m.
Aspen Clubhouse, Willow Room

Scams can be so convincing. We want to show you what to look for to determine if you are being scammed and how to fight back by reporting them. You can protect yourself when you understand how scammers work.

New members may join at any time.
We have a \$15 annual club fee. Pay in person at any meeting or put your check in Box C by the Aspen front desk.

More Information can be viewed online
savcc.net
Or call Kim VanDorn SAVCC President at:
(760) 954-5946



Multi-Factor Authentication

Cookies

Phishing:

Grandparent scam

Virus

Artificial intelligence

Trojan horse

Hacker

Spyware

Identity theft



Robocall

Malware

Skimming

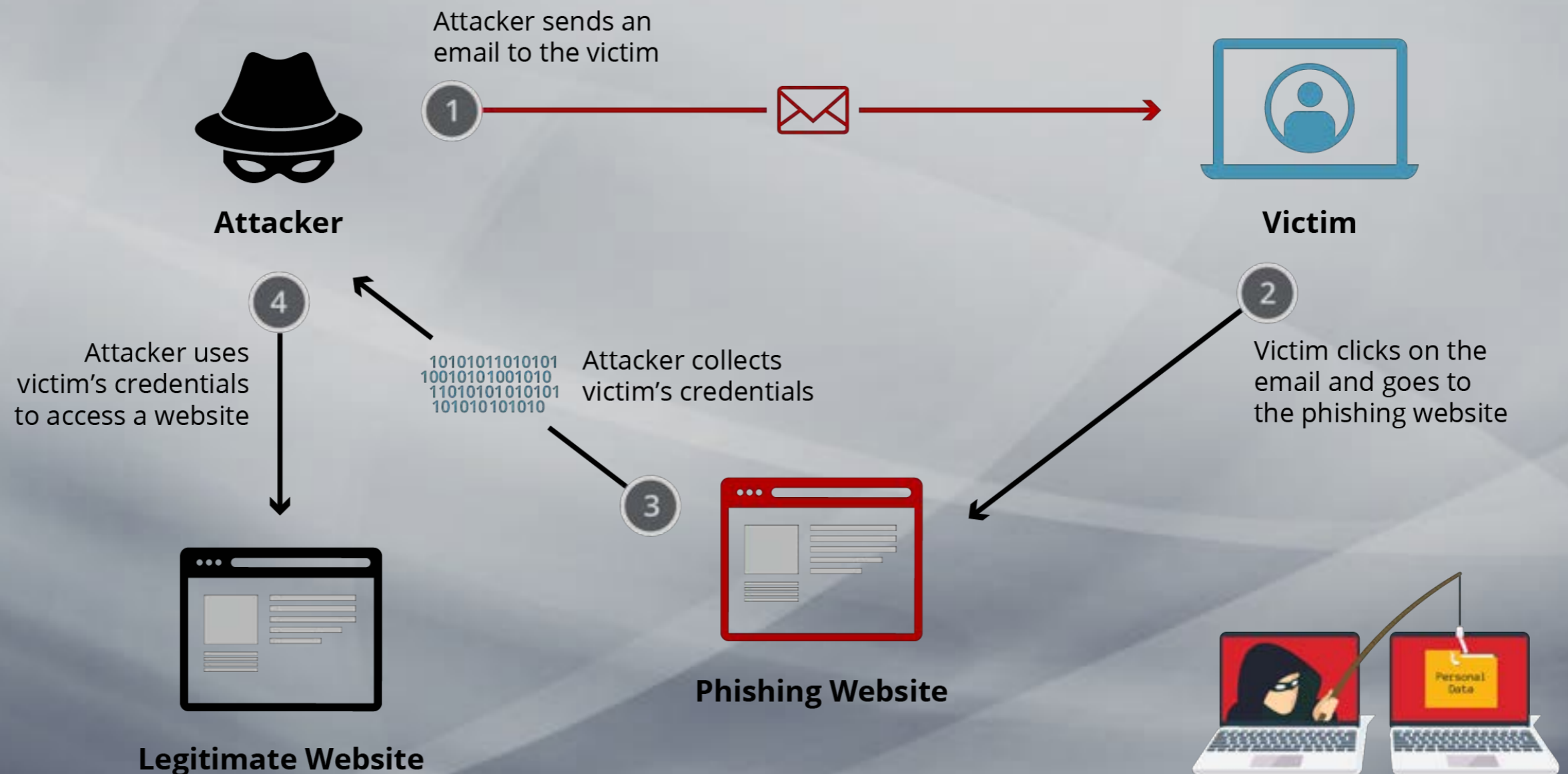
Ransomware

Let's define some often used words.

Scamming

Scamming, in the context of computers refers to fraudulent activities where cybercriminals attempt to deceive individuals or organizations. Here are some common types of computer scams:

1. Phishing: Scammers use email, phone calls, or text messages to pose as legitimate entities (such as banks, tech support, or government agencies) and trick victims into revealing sensitive information like passwords, credit card details, or social security numbers. Phishing relies on human error and manipulation to succeed.



When in
doubt,
Throw
it out!!!

Watch for these five red flags of phishing in emails, calls, and texts:

1. They ask you to open a link.
2. They use urgent or fear-inducing language.
3. They send an attachment.
4. They request personal info like PINs, passwords, or social security numbers.
5. They pressure you to log into, or send money with, payment apps.

All Inboxes
42 messages, 25 unread

Filter Archive Delete Junk Reply Reply All Forward New Message Get Mail Smaller Bigger Search

All Inboxes

Package Inbox - iCloud 5:34 AM
Your Shipment Status Update...
Tracking Alert: Your UPS Package is Making its Journey unsubscrib...

Trump EXPLO... In... 5:34 AM
Must see: HUGE move for Pr...
»Kathy, drop everything you're doing right now. Click here to un...

Lectric eBikes Inbox... 5:31 AM
You Can Go the Distance
Range anxiety? Shop our long-range XP 3.0 eBikes & Save \$60,...

The Discoverer Inbo... 5:29 AM
10 Unspoken Rules of Travel...
Inspiration for your future travels, curated and delivered daily. 10 Un...

L.L.Bean Inbox - iCloud 5:18 AM
Gifts That Are a Joy to Give, An...
Favorite gifts for your favorite people, all in one place. View this...

Big Lots Inbox - iCloud 5:15 AM
25% off ALL holiday candles...
Plus, more BIG DEALS inside! View small in your browser *Our *com...

The Daily Press Inb... 5:02 AM
The latest issue of The Daily...
Thursday, November 16, 2023 Click below to read today's paper. Shu...

Package ✓ abercrombie@kiolma.operationbim.com
Your Sh...
To: Kat...

Copy Address
Add to VIPs
Block Contact
New Email
Add to Contacts
Search for "Package"

Inbox - iCloud 5:34 AM

Tracking ... is Making its Journey

You have (1) package waiting for delivery.
Confirm your shipping details
CONTINUE

Schedule your delivery and subscribe to our push notifications to avoid this from happening again!

Your tracking code:
IPHON-772-H9B5

Amazon Suggestions

When in doubt,
Throw it out!!!

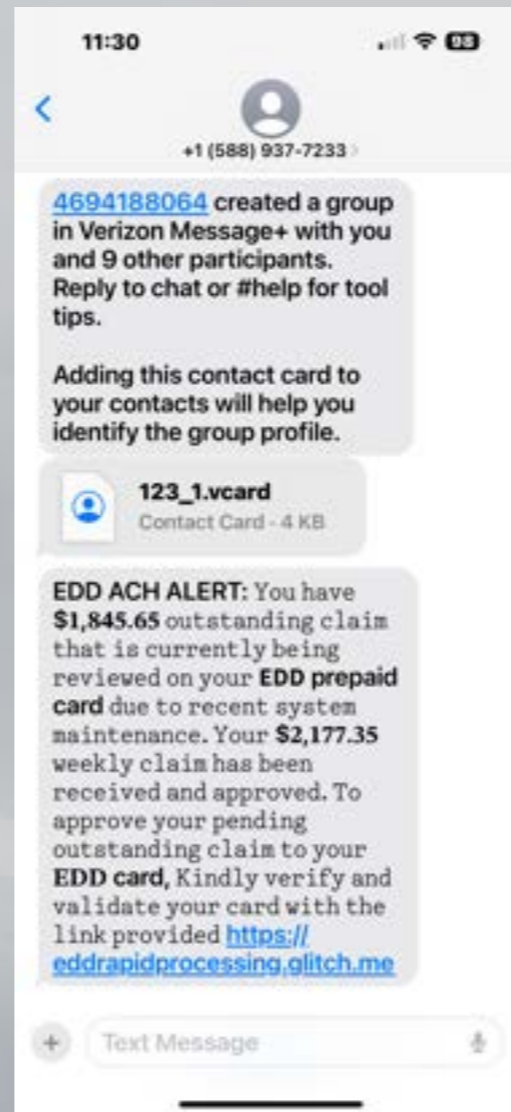
1. Look for unusual email addresses.
2. Misspelled words.
3. Suspicious URLs to link to
4. Unexpected attachments. (May contain malware.)
5. Don't scan a QR code you aren't expecting. And check URL when you do.



Also:

Smishing: Smishing is phishing that takes place via text message, also called SMS. Because fraudsters can spoof phone numbers, smishing scams can be convincing and may appear to come from trustworthy senders. In fact, the fraudster may be after your personal information or could try sending you a virus.

When in doubt,
Throw it out!!!



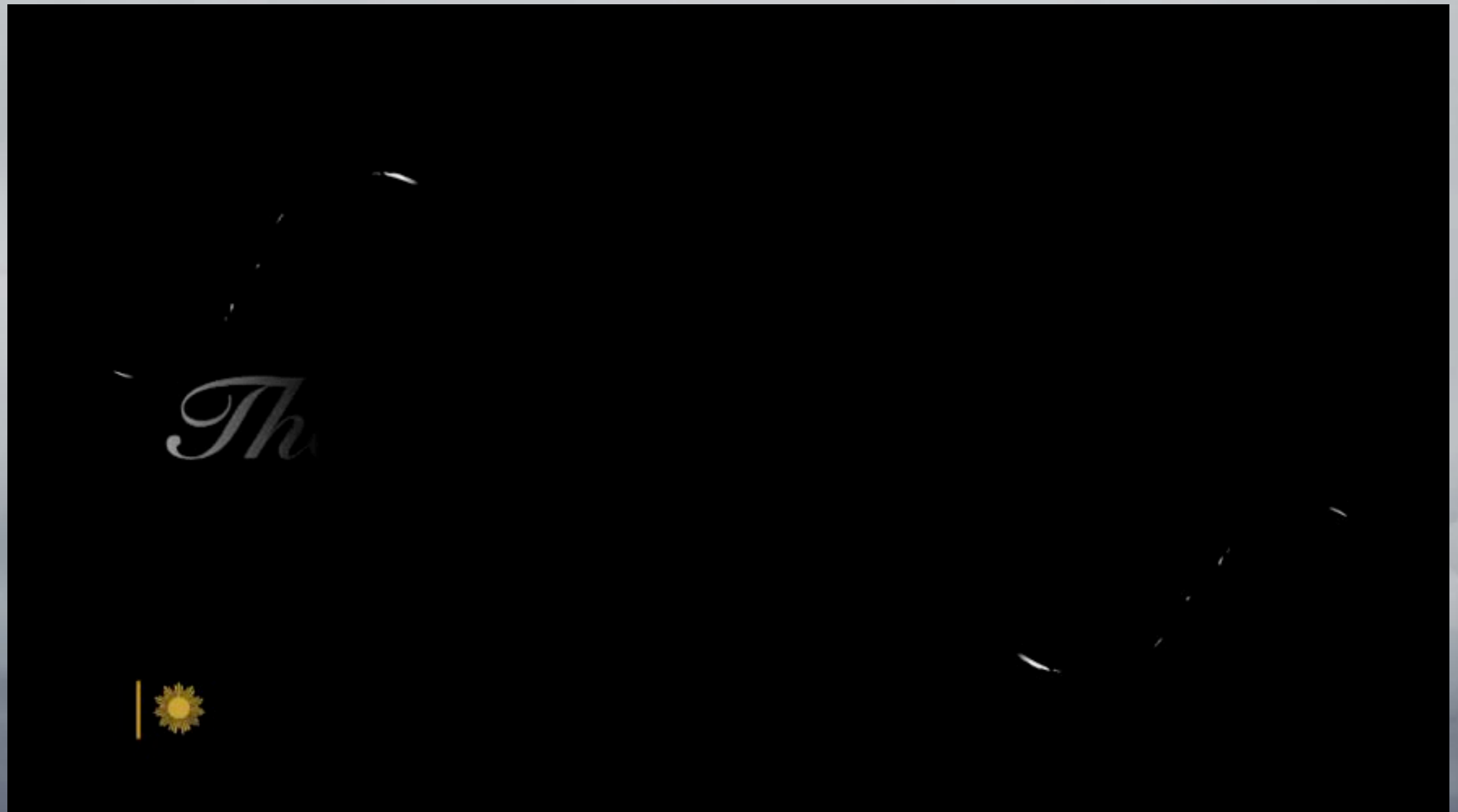
1. Comes from strange phone numbers
2. Has an urgent warning request.
3. Requests personal information.
4. Odd grammar or spelling mistakes.
5. Suspicious links.
6. Don't scan a QR code you aren't expecting, and check URL.

Vishing: Vishing, although mostly done by phone, is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers: many victims of vishing are people who are not tech-savvy.

2. Impersonating: Scammers often try to convince their targets to send money via a wire or money transfer. Although this is done over the phone, new technologies using AI or artificial intelligence is now easily able to clone a persons voice so that it sounds just like your “granddaughter”. They can find an audio clip on social media or elsewhere on the internet. All they need is as little as 3 seconds, 10 seconds is even better to get a very realistic clone of your voice. The audio sample is then run through an AI program that replicates the voice, allowing the scammer to make it say whatever they type in addition to adding laughter, fear, and other emotions into the cloned voice depending on how the scam is scripted. Always hang up and call the person directly if in doubt.



3. Tech Support Scams: Scammers pretend to be tech support representatives and claim that the victim's computer has issues. Issues can be sited through browsers, emails, text or phone calls. They then request remote access or payment for fake services.



So What can you do?



Let's talk with samples...

Is your head spinning yet?



A few more things you need to know...

Should I accept cookies?

Cookies

Computer cookies, also known as HTTP cookies, internet cookies, or browser cookies, are simply small packets of data that a computer receives from a web server and sends back without alterations. These cookies play a crucial role in web browsing and online interactions. Let's dive deeper into what they are and how they work:

1. What Are Cookies?

Computer cookies are small files used by web servers to save browsing information. They allow websites to:

- Remember your device.
- Store browser preferences.
- Track associated online activity.

2. Types of Cookies:

Persistent cookies: These can save data for an extended period, such as storing username and password information for users.

Third-party cookies: These collect data about your online activity to improve advertisements.

Session cookies: These delete immediately after closing your browser and are commonly used for features like maintaining items in a shopping cart.

3. Safety and Privacy Considerations:

- Under normal circumstances, cookies cannot transfer viruses or malware to your computer.
- However, some types (like "supercookies" or "zombie cookies") can be potential security concerns.
- Third-party tracking cookies may compromise privacy by allowing unidentified parties to monitor your online behavior.

4. Managing Cookies:

Most browsers allow you to manage cookies easily:

- Open your browser settings.
- Navigate to where cookies are stored (location varies by browser).
- Clear browser data or manage cookies as needed.

Remember that cookies can benefit both users and websites, but understanding their implications is essential for privacy and security.

Google

Good to know



Home | Living the Dream \$10K Giveaway



Thank You for Entering! Visit [HGTV.com](https://www.hgtv.com) for a second chance to win! Enter twice daily - once on FoodNetwork.com and once on HGTV.com through April 17th, 2024 at 8:59 a.m. ET.

Enter Again at [HGTV.com](https://www.hgtv.com)

Indulge Your Tastebuds




Dreamy Dishes



GET YOUR GUIDE

Keukenhof: Flower Fields Small-Group Cultural Bike Tour

from \$51.48 [Book now](#)




Likely to sell out

from Lisse: Flower Bike Tour Along Keukenhof and De Tu...

from \$48.77 [Book now](#)

Keukenhof
Home Ontdek het park Plan uw bezoek Veelgestelde vragen Contact
Bestel tickets




Keukenhof
Powered by

Consent
Details
About

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our usage. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Should I accept Permissions and Locations Services?

Avoid Unnecessary Permissions:

- Only grant permissions that are necessary for the app to function properly.
- Be cautious with permissions related to sensitive data (e.g., camera, microphone, location). If an app doesn't need access to something, don't allow it.

Remember to review app permissions carefully and prioritize your privacy when deciding whether to accept or deny them.

Location Services:

- Enable or Disable: When you set up your iPhone, you're asked if you want to turn on Location Services. You can also enable or disable it later in Settings > Privacy & Security > Location Services.
- App Requests: The first time an app wants location data, you receive a request with an explanation. Some apps may ask for one-time access, while others may request ongoing access.
- Review and Change Access: You can review or change an app's access to location information in the same settings. Leave "Precise Location" on to allow specific location access or turn it off for approximate location sharing.
- Third-Party Apps: Be aware that third-party apps' location usage is subject to their terms and privacy policies.
- Remember, turning off Location Services may affect important iPhone features. Always review app permissions carefully.

On Your iPhone: Discoverable By Others In Journaling App

Last year, [as a part of iOS 17.2](#), Apple released the Journal app. You can use it to jot down personal notes about your day, your life, what inspires you. You know, journal-y things.

You can turn on Journaling Suggestions. This recommends topics to write about based on things your phone (but not Apple) knows about you—music you’ve listened to, people you’ve called or messaged, photos you’ve recently taken, places you’ve visited, etc. You decide if you want to turn this on. When you first launch the Journal app, it will prompt you to do that. Those suggestions aren’t ever shared with Apple.

Here’s where it gets weird. When you go into Settings > Privacy & Security > Journaling Suggestions, you’ll see that Discoverable by Others is enabled by default—even if you never turned on suggestions. Under the setting it says, “Allow others to detect you are nearby to help prioritize their suggestions.”

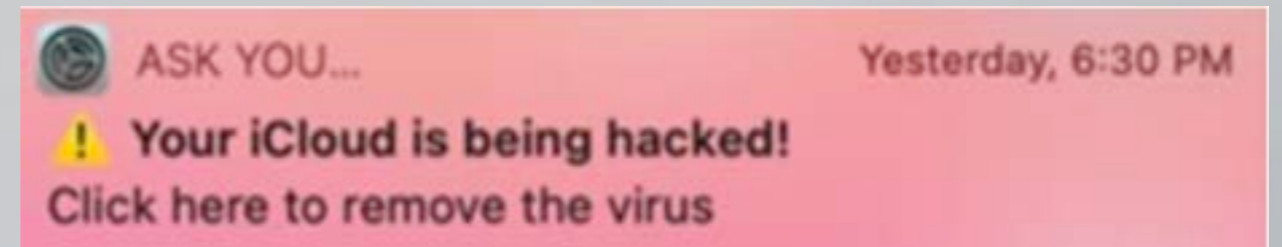
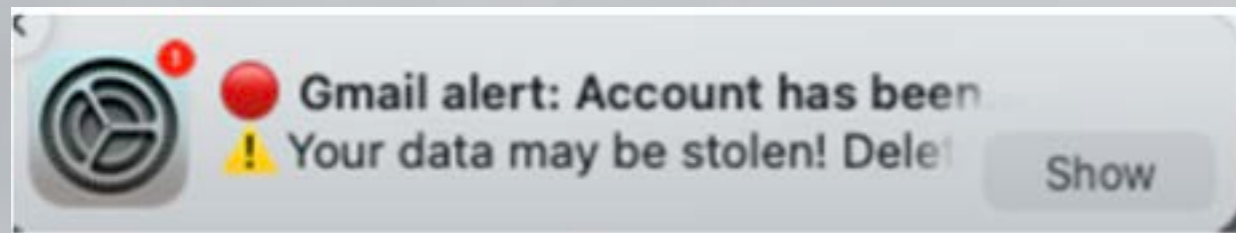
Uh. Why is this on by default when the suggestions setting is off by default? Is the iPhone automatically reminding my nearby contacts that I am around? And encouraging them to journal about what we are doing together?



How to stop fake System notifications on macOS

Posted: November 21, 2023 by [Pieter Arntz](#)

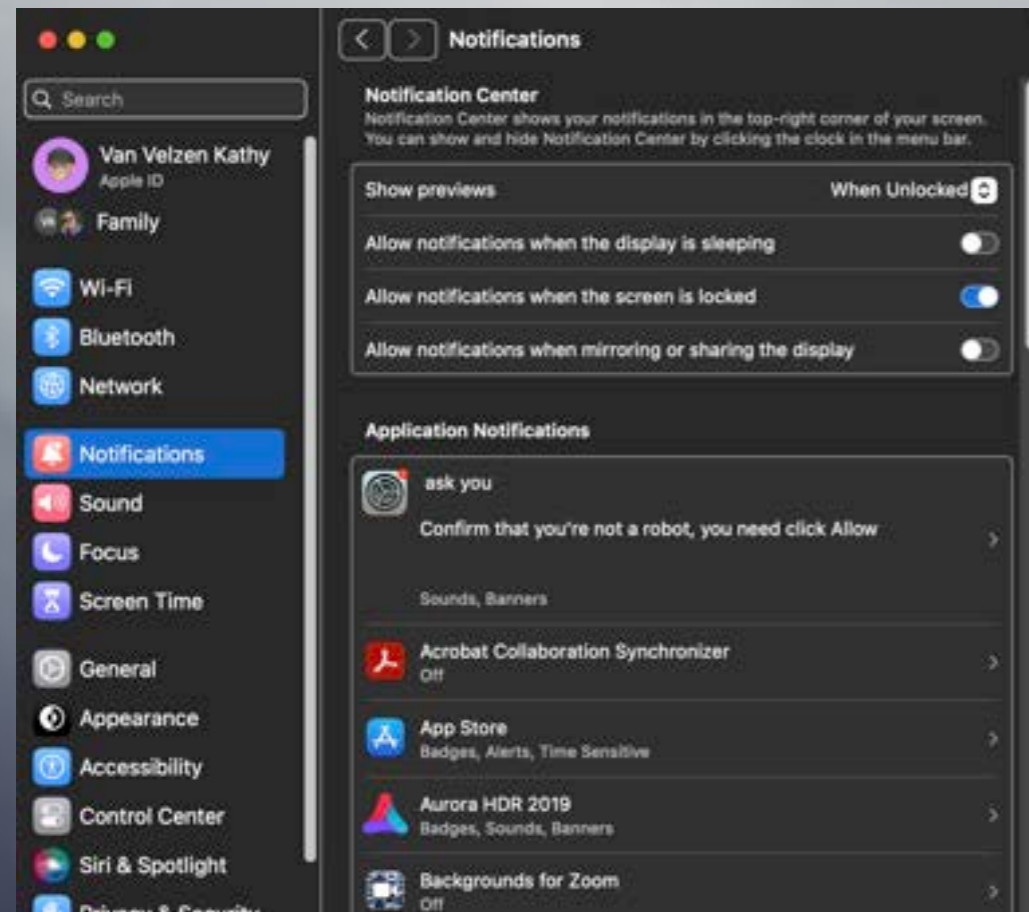
Scammers are abusing an Apple feature that allows websites to create push notifications that look like they're coming from macOS, or apps. The notifications try to scare users into clicking a link with fake virus alerts or messages saying their account has been hacked.



Open your Apple **System Settings** and then select the **Notifications** tab along the left.

Scroll down the list under **Application Notifications** and look for any websites that have permission to send you notifications. The entry may have a name designed to mislead you, such as “ask you” or “Notifications”.

Under each item you will be able to see what type of notification permissions it has. To stop these, just click on the entry and turn off the slider at the top which will disable notifications for this item.



Safari Settings

In the Safari app on your Mac, choose **Safari** and click **Settings**. Click **Websites**, then click **Notifications**.

Scroll through the list of websites and look for websites that don't want to receive notifications from. Anything that shows **Allow** can send you messages, so switch them to **Deny** if you do not want to see their messages.

Multi-Factor Authentication

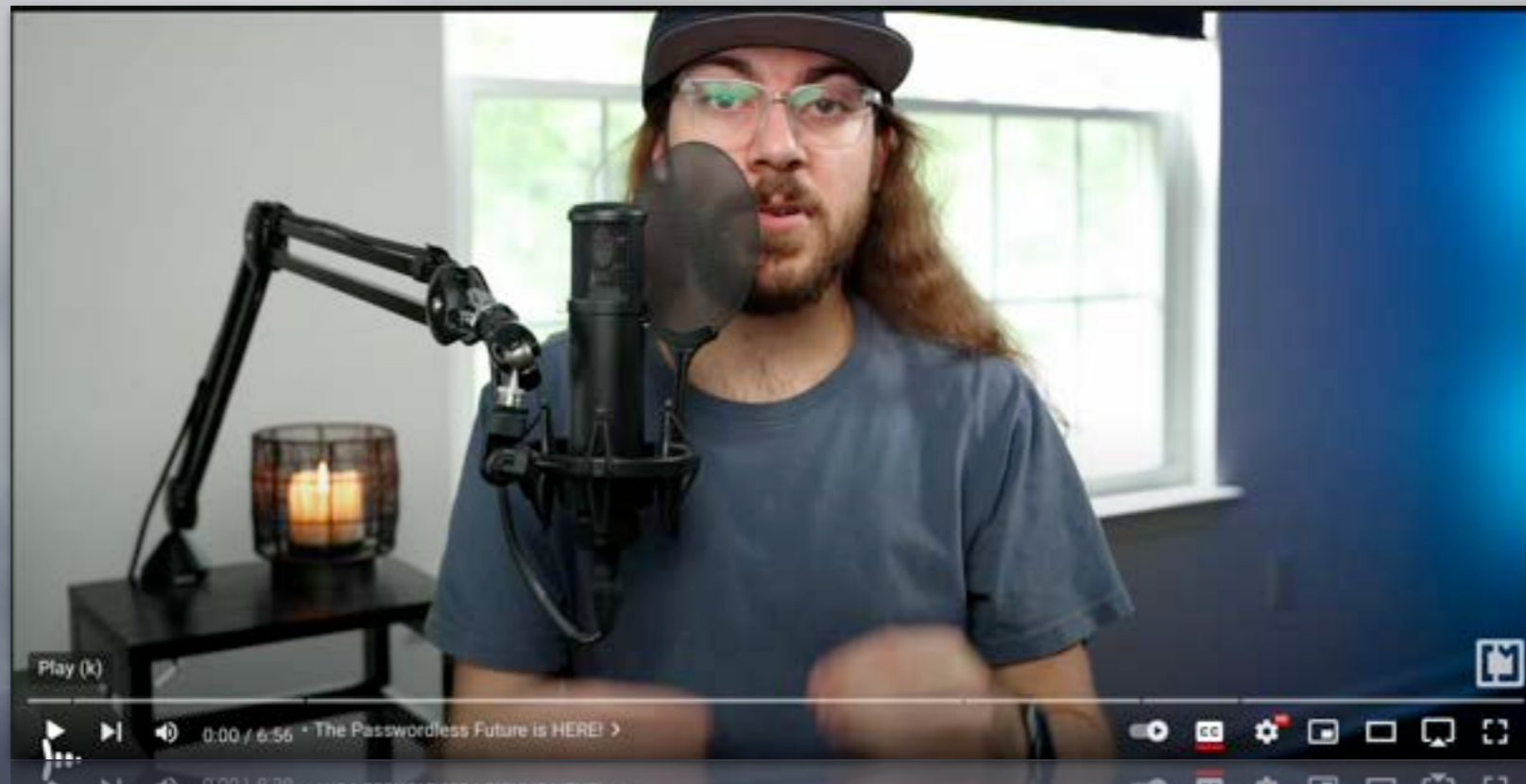
Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy.

Here are the three main types of MFA authentication methods:

1. Things you know (knowledge):
 - Examples: Answers to personal security questions, passwords.
2. Things you have (possession):
 - Examples: One-time passwords (OTPs) generated by smartphone apps, OTPs sent via text or email, access badges, USB devices, smart cards, or security keys.
3. Things you are (inherence):
 - Examples: Biometrics such as fingerprints, facial recognition, voice, retina, or iris scanning.

MFA enhances security by requiring users to identify themselves using more than just a username and password. It decreases the likelihood of successful cyber attacks and provides increased confidence that organizations will stay safe from cyber criminals.

Passkeys For The Future Instead of Passwords

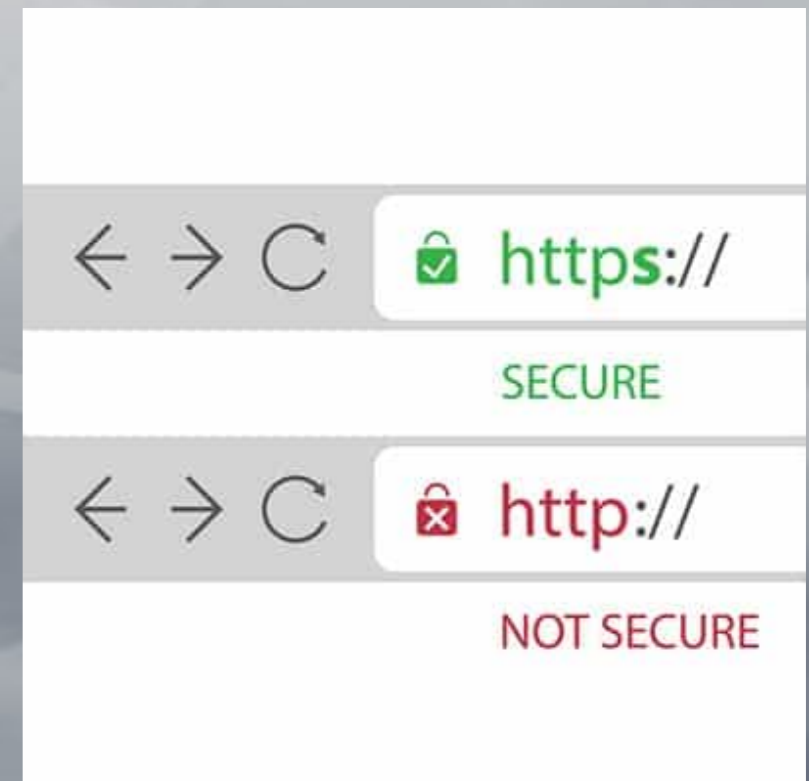
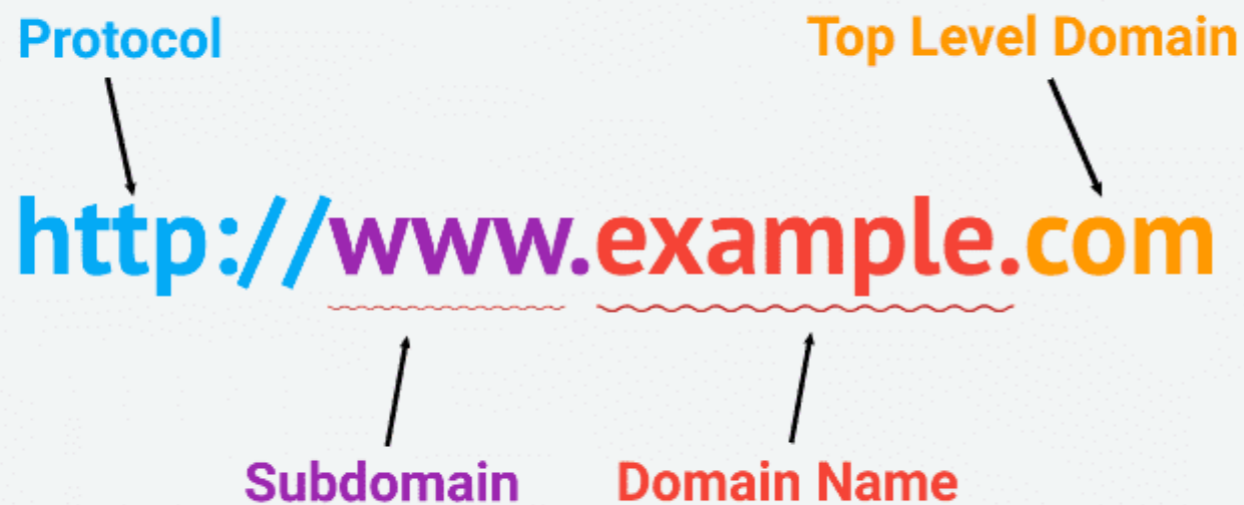


Secure Websites

When conducting money transactions online, it's crucial to ensure the security of the website. Here are some tips to help you identify a secure website:

1. Check the Website URL: Look for a web address that begins with "https://" instead of just "http://". The "s" indicates a secure connection.
2. Padlock Icon: Check if there is a padlock symbol in the browser's address bar or the lower-right corner of the webpage. This indicates that the website has a secure connection.
3. Use Reputable Third-Party Services: Whenever possible, use trusted third-party services like [PayPal](#) for online transactions. These services provide secure transactions and dispute resolution.

Remember to stay vigilant and protect your financial information while making online payments!



And Lastly...

Malware. Short for [malicious software](#), this term encompasses computer viruses and other types of programs that cybercriminals use to disrupt or access your computer, typically with the aim of gathering sensitive files and accounts.

Malvertising. [Online advertising](#) that contains malware activated when you click on the ad.

Spyware. A type of malware installed on devices to track your actions and collect information without your knowledge.

Ransomware. Malicious software that restricts or disables your device or may hijack and encrypt files, then [demands a fee](#) to restore the device's functionality.

SIM swaps. Thieves may either convince your cellphone carrier to transfer your number to the thieves' phone and existing SIM card or they may claim your SIM card has been damaged and get a replacement card sent to them. Once in possession of a [SIM card](#) associated with your phone number, the thieves may be able to access your credit card, bank and other financial accounts.

Call spoofing: Call spoofing, also called neighbor spoofing, is when a fraudster falsifies the information that shows up on your phone's caller ID. A scammer could use this tactic to more convincingly pass themselves off as someone you might know or as the Social Security Administration or some other government agency.

How to Protect Yourself From Scams

While it's true that phishers use increasingly sophisticated techniques to steal information, it's also true that you can avoid many of their attempts if you know what to look out for. Here's how to protect yourself from identity theft and reduce the risk of being targeted.

Guard Your Personal Information

Immediate requests for money transfers or for your Social Security number are a sure indication that you're dealing with a scammer. Avoid phishing scams by safeguarding your sensitive information.

Don't give out your Social Security number or bank account number to anyone who calls and asks you for it. A legitimate banker or government official won't call and request this information. If someone you think is official calls and asks you for identifying information, hang up and call back using the number listed on the organization's official website.

Set Up Strong, Unique Passwords

Using the same password across your devices and financial accounts places you at a higher risk of losing your key information to a fraudster.

Instead, use unique and complex passwords with a combination of letters and numbers. Using a password manager can be an easy way to securely keep track of your passwords.

Review Your Credit Reports Regularly

Make it part of your routine to regularly check your credit reports for discrepancies. You can get free copies of your credit reports from all three major consumer credit bureaus at AnnualCreditReport.com. You can check your Experian credit report and credit score for free through Experian.

If you encounter information you believe may be the result of fraud, dispute the information with the appropriate credit bureau right away.

Handle Sensitive Mail Responsibly

Check your mail every day and bring all letters inside to help prevent mail theft. Shred anything with personally identifying information on it before tossing it, and store documents you intend to keep in a secure place.

You can also opt out of credit offers and choose to receive electronic statements from your utility companies and credit issuers to limit the amount of sensitive mail you receive.

The Bottom Line

Scammers thrive on surprise—an alarming phone call, a confusing message, a threatening letter, a malicious link in an innocuous email. If you know what to expect and stay up to date on the tactics of scammers, you'll be much harder to target.

If you're worried a scammer has accessed your information, you can place a fraud alert on your credit reports. The alert asks lenders to confirm your identity before issuing you any new credit. If you've repeatedly been victimized by scammers, you might consider securing your credit with a credit freeze, which blocks access to your credit history.

Lastly, report any attempts at phishing using the Federal Trade Commission's official reporting site to help law enforcement track and prevent identity theft.

Sweet Dreams....

