Scammers

Clay E. Olsen
clayeolsen.com
Version 1.8 – 29 December 2023

Background

- I will walk through examples using Yahoo's email client and REI's website. The yahoo email address is for example purposes only.
- I want to stress that these attacks can happen with any email provider, such as Gmail, Hotmail, Outlook, etc.
- I also want to stress that any website can be hacked. What happens to REI in these examples could happen to Etsy, Pinterest, Amazon, and others.
- Websites are constantly being probed by hackers looking for flaws. Some of these flaws allow them to gain access to information they should not be able to access.
- There will never be a perfectly secure website or email client.

Example

- A person creates their first email account: IamTheHappyCamper@yahoo.com
- This person then goes to REI's website, a camping co-op store, and creates an account there so they can buy camping gear. They provide their name, address, phone number, credit card, the Happy Camper email address, etc. They make a large purchase.
- Two years have passed, and they haven't needed any more gear, so they haven't used REI's website. However, their account remains on REI's website.

The website hack

- A hacker finds a flaw in REI's website that allows him access to the email addresses associated with REI's customer accounts. The flaw was not severe enough to allow access to credit card information and passwords.
- Due to the flaw, the hacker can access 100,000 email addresses from REI's customer accounts. The hacker saves these email addresses.
- The hacker sells all 100,000 email addresses to BadGuyPhish for 5 cents each and tells them they came from REI's website.
- BadGuyPhish gets to work.

Phishing

- BadGuyPhish will create an email that looks a lot like an email from REI.
- The email may state, “Your payment information is outdated. Please update your credit card to avoid your account being closed. For your convenience, click here.”
- Your email address is one of the 100,000 that BadGuyPhish purchased. He sends you this fake email. This technique is called Phishing – trying to find a fish – a naïve player - like a Texas Hold ‘Em poker pro who finds someone who thinks they are good at poker and has a lot of money.
- Since it has been two years and the email looks authentic, you realize that your credit card is probably outdated, so you click the link and provide your updated card info.

Selling Credit Card Numbers

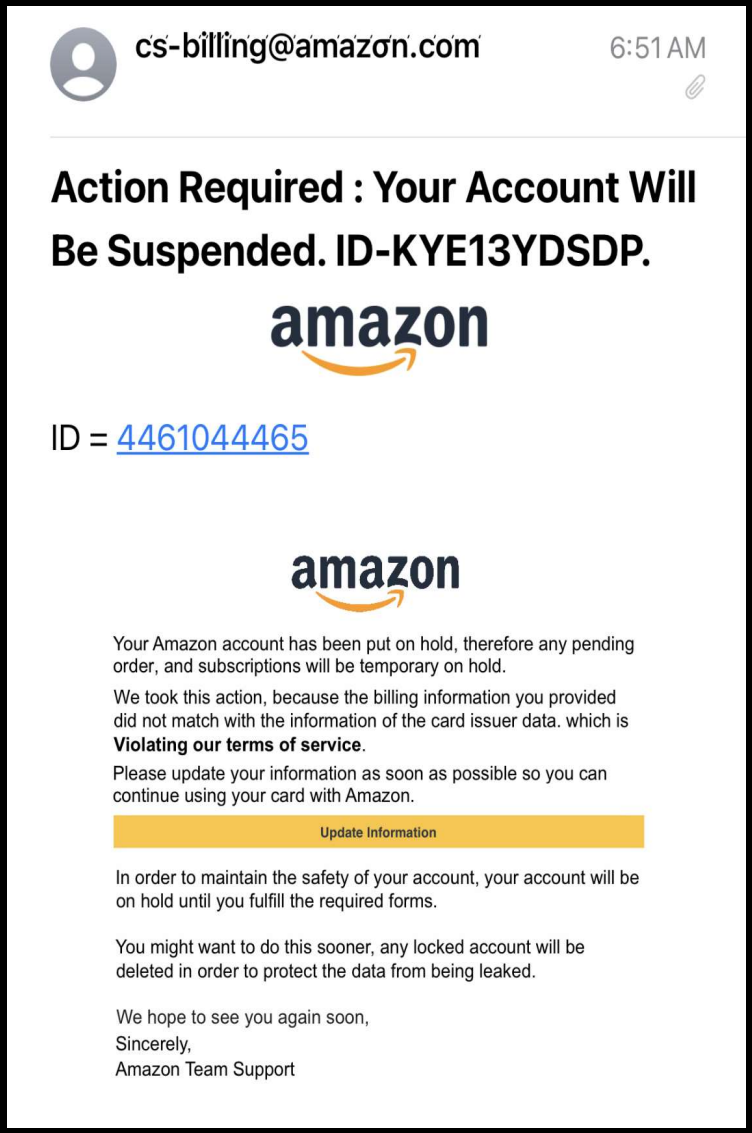
- By clicking the link in the email, you weren't taken to REI's website. You were at BadGuyPhish's website, which he made to look exactly like REI's website. Instead of providing your credit card info to REI, you really provided it to BadGuyPhish.
- Out of 100,000 emails, BadGuyPhish was able to trick 10,000 people into giving up their credit card numbers.
- BadGuyPhish doesn't have a credit card fraud infrastructure, so he sells the credit card numbers to someone who does at $5 each. His profit: $45,000.

Not Done Yet....

- Our original hacker knows that most people have only one email address. What are the odds that this email address is used for Amazon, Apple, Microsoft, Etsy, PayPal, Ancestry, and so forth?
- Our hacker sells these email addresses to other BadGuys who will also attempt to phish these accounts.
- Except for creating the phishing email and a similar website, computers handle the rest, so it is a very low-cost, high-reward attack.
- More profit, less cost.
- Let's look at a couple of these emails….

Amazon Example 1

- Looks legit, but it is not.
- English isn't very good: "until you fulfill the required forms." and "you might want to do this sooner, any locked account will be deleted in order…" Double Whammy! Unsolicited + Urgency.
- At some point, these people will begin using AI and grammar checkers, making these errors much harder to spot.



cs-billing@amazon.com 6:51 AM

Action Required : Your Account Will Be Suspended. ID-KYE13YDSDP.

amazon

ID = 4461044465

amazon

Your Amazon account has been put on hold, therefore any pending order, and subscriptions will be temporary on hold.

We took this action, because the billing information you provided did not match with the information of the card issuer data. which is **Violating our terms of service**.

Please update your information as soon as possible so you can continue using your card with Amazon.

Update Information

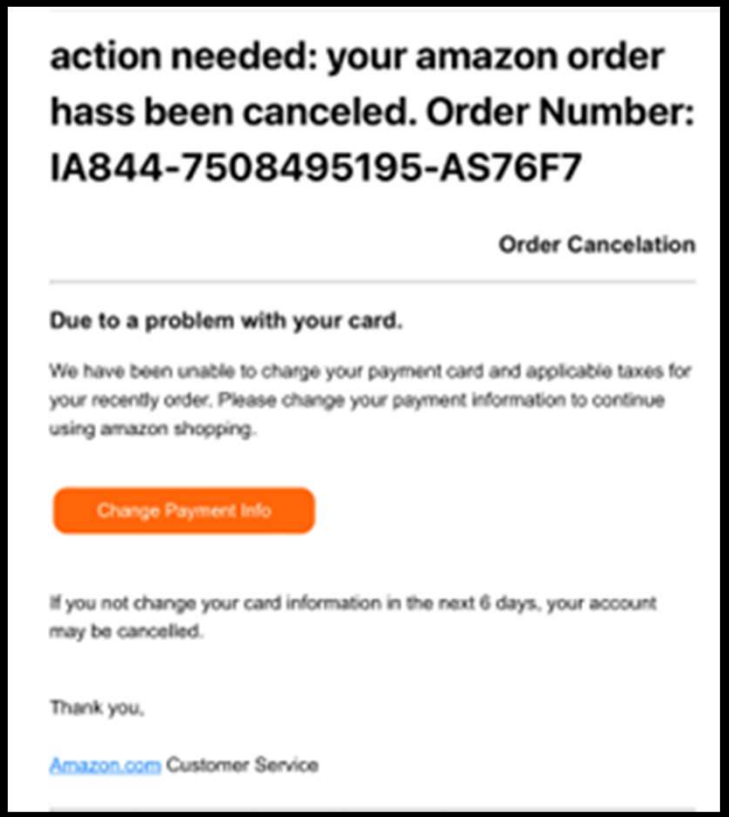
In order to maintain the safety of your account, your account will be on hold until you fulfill the required forms.

You might want to do this sooner, any locked account will be deleted in order to protect the data from being leaked.

We hope to see you again soon,
Sincerely,
Amazon Team Support

Amazon Example 2

- This technique worked great during COVID when shipping was slow, even if the English was bad.



action needed: your amazon order hass been canceled. Order Number: IA844-7508495195-AS76F7

Order Cancelation

Due to a problem with your card.

We have been unable to charge your payment card and applicable taxes for your recently order. Please change your payment information to continue using amazon shopping.

Change Payment Info

If you not change your card information in the next 6 days, your account may be cancelled.

Thank you,

Amazon.com Customer Service

What if the REI hack did get the passwords?

- Let's assume the flaw in REI's website was severe enough that the hacker got email addresses and passwords. Fortunately, the passwords are not stored "in the clear" like email addresses.
- Passwords are put through a one-way hash function. They are represented as a large numerical value. The same password will hash to the same numerical value.
- What the hacker will have access to is the email address / hashed-password combination. This hacker sells the email address / hashed-password combination to BadGuyMalware.
- BadGuyMalware has databases full of common passwords and their equivalent password hashes. He searches for a match. If he finds a match, he knows the "in the clear" password – the password you type in when you log in.

Passwords: Two Big Problems.

- The first big problem is using poor passwords. Unfortunately, many people believe things like “123PASSword456!” or “!QAZxsw2” are strong passwords. They are not. BadGuyMalware, with his hashed password list, will find them immediately
- The second big problem is that people use the same passwords for multiple accounts. Why is that a problem? Well, let’s see what happens

Two big problems lead to one MAJOR problem

- In this attack, BadGuyMalware purchased the REI email address/password hash list from the website hacker. He searches his password hash list against the hashed password. He finds a match for it and now knows the "in the clear" password is "123PASSword456!"
- He also knows the email address is IamTheHappyCamper@yahoo.com. He goes to yahoo.com and enters "IamTheHappyCamper" as the username and "123PASSword456!" as the password. BOOM – he is in! It works because Happy Camper used the same password for REI as he did for his email account. BadGuyMalware now has complete access to Happy Camper's email account.

Exploiting trust

- BadGuyMalware has compromised Happy Camper's email account. He goes through the "Sent Items" in the email client. He finds some old messages where pictures were exchanged between Happy Camper and his friends.
- He sets up a new email account: IamTheHappyCampar@yahoo.com with the display name "Happy Camper". Notice how it is Campar, not Camper.
- He crafts an email that includes text from one already sent. He will send this email to each person individually. Because it contains text from an authentic exchange, it comes from an email address that looks almost exactly the same and has the display name of "Happy Camper," his friends will think it came from Happy Camper

The Malware Attachment

- BadGuyMalware attaches a FamilyJPG.ps file to the email and sends it out with the message “new family pic!” When the user receives the message, they think it is from their friend or family member. They automatically click on the attachment. Nothing happens they can see. However, a keystroke logger is silently installed in the background on their Windows PC.
- From now on, everything the friend types on their keyboard is secretly sent to BadGuyMalware. Things like their usernames/passwords and the financial institutions they belong to.
- The friend replies to the email message – “Your picture didn’t come up!” – but that reply is going to IamTheHappyCampar@yahoo.com, not IamTheHappyCamper@yahoo.com. Weeks later, the friend talks to Happy Camper on the phone, and Happy Camper says, “I didn’t send any picture out – what are you talking about?” By that time, the damage is done.

An uncomfortable truth about Anti-Virus Programs.

- Someone may say: “Hey, my anti-virus scans all my email attachments, so this attack won’t work against me.”
- In general, anti-virus programs are good to have. I personally use Windows Defender (free). Sometimes when I’m helping someone disinfect their PC, I have to pull down other programs.
- However, anti-virus programs can only search for KNOWN attacks.
- BadGuyMalware may have developed an attack that anti-virus companies don’t know about yet, and software companies don’t know about it either, so no fix is available (these are called Zero Day attacks).
- Also possible, BadGuyMalware used obfuscation techniques to hide a known attack and get it past anti-virus programs.

Another Attack - Ransomware

- Typically, ransomware is delivered via a malware attachment or via a link to a malware website (e.g., a user clicks on a link in an email).
- Ransomware encrypts your drives, so you can't access any information on them. The attacker demands a ransom. Once the ransom is paid, the attacker will decrypt your drives. That is the only way to access your photos and other personal items. Depending on what is on those drives, the attacker may have some leverage over you and threaten to post the content publicly.
- A small business can be put out of business with this attack. Imagine all your client data (e.g., real estate clients, dentist patients, etc.) is encrypted with no way to access it except by paying a lot of money.
- A ransom amount may be six figures for a small business.

Yet Another Attack - Gift Card Requests

- Assuming that BadGuyMalware has compromised your email account, he can execute another attack.
- He sends an email to you pretending to be one of your friends. It says, “I’m stuck in a Mexican jail and must pay the police to get out. The corrupt Mexican police will only accept gift cards since they are not traceable!”
- Several variations are possible – unexpected medical bills, accidents, etc.

More Problems Due to Password Re-Use

- BadGuyMalware is not done. What if HappyCamper used the same password for Amazon, Paypal, Facebook, and so forth?
- Although credit cards are blanked out except for the last four digits, the amount of information that BadGuyMalware can get is pretty impressive. This information can be used to generate sophisticated attacks.
- Compromised accounts can be sold to other hackers as well.
- Hackers use compromised accounts to generate likes for pages/products on Facebook falsely, post favorable product reviews, run secret Facebook advertising campaigns, and other bad things.

Another way to compromise your accounts: Account Recovery Attacks

- Sometimes, we change our password and forget the new one. To get back into our account, we must go through an Account Recovery process.
- Account Recovery may ask you for a previous password. If you know the previous password, then they'll ask you the security questions you answered when you set up the account – like "What is your mom's maiden name?"
- Other platforms, such as Facebook, may have additional account recovery options, such as recovering your account through one of your Facebook friends.
- Attackers can pretend to be you and "recover" (i.e., take over) your account.

More Personal - Phone Calls

- If your phone number gets out, you may get calls over your phone, similar to what you get over email.
- Examples: Someone from Microsoft claims your Windows computer has a virus. Social Security calling that your benefits are on hold. Hackers claiming to be public utility companies in your home town and the service would be shut off unless they got a credit card number.
- Also, recognize that everything you see in your “Caller ID” can be faked.

An Even More Personal Attack - Natural Disasters

- Most people don't have a high opinion of attorneys that chase ambulances. There is something worse. Scammers often follow insurance adjusters to natural disaster locations.
- Usually, they'll wait a bit until the insurance companies have cut checks. Then they come in with low-cost deals. Roof repair? I can replace your roof for $5500. Wow – everyone else wants $10,000.
- Some folks demand the material to show up before paying half the amount. The scammer then steals the material from a legitimate roofing company at night and then places it on the customer's front lawn. They say they'll get started in a few days. They take half the money and never return.

How do we fight back? Some Complications...

- Sadly, many legitimate companies send emails with links for your convenience. For example, credit card companies will send you your balance and a link to pay your bill online.
- If you purchase something, the company will often send you tracking information, which is typically a link in an email
- Some companies will send you a PDF invoice, return address labels, and so forth as attachments via email.
- Friends get new phones. You may even get a new phone number.
- Sometimes, things are urgent.

The Uncomfortable Truths About Being Online

- The more your online experience is convenient for you, the easier it is for hackers.
- The more your online experience is inconvenient for you, the more challenging it is for hackers.

Rule #1
Unsolicited + Urgency + Email = Fraud

- Beware of an unsolicited email trying to create a sense of urgency, especially around an account (e.g., Amazon).
- Everything contained in the email is designed to fool you.
- When I receive such an email, I typically bring up the application on my phone or tablet (e.g., Amazon, eBay, etc.). I then check if I have any notifications in their application. This way is the best way to check for any problems with your account. If you don't have an application handy, you can use a browser and type in the website (e.g., www.amazon.com, www.ebay.com, etc.).
- If you are concerned that the claim may be legitimate, you can call the company (using a phone number you looked up, not a phone number from the email), chat with support in the browser (after you typed in the website), or stop by the office if it is a local company.

Rule #2

Unsolicited + Urgency + Phone = Fraud

- Water, gas, or electric companies calling on the weekend saying they will shut you off.
- Social Security Administration saying your benefits will be frozen.
- Don’t say anything. Just hang up. Look up the company number (i.e., electric company, social security, or whatever), call them, or stop by the office.
- Don’t call the number on the Caller-ID. It is fake. Just like the Caller-ID description. There are ways to manipulate this information.

Rule #3

An online business or person that won't take money orders OR credit cards = FRAUD

- Don't buy things online with a person or business that only accepts Zelle, Venmo, Gift Cards, etc.
- They'll probably say they accept those methods to keep costs down. WRONG. Companies now charge credit card transaction fees and pass those on to you. Credit cards should cost nothing for them to use.
- Alternatively, they may say they've been cheated by other methods. RIGHT….

Rule #3 - continued

USPS Money Orders

- I've successfully used USPS money orders for those sellers that require money orders.
- If I purchase something online and I'm going to send a USPS money order, I require the seller to have a physical address. No physical address, no money order.
- I put the USPS money order in an envelope, then place it in a priority mail envelope and set the appropriate restrictions on it (signature required, etc.)
- You can check priority mail tracking and the USPS money order status (whether it was cashed or not) via tools on the USPS website.
- Be sure to save your USPS money order receipt and your USPS receipt for the priority mail with the tracking info until you receive your product.

Rule #3 - continued

An online business or person that won't take money orders OR credit cards = FRAUD

- Money orders and credit cards are the two safest methods for the buyer and seller. A seller may only accept money orders but not credit cards. Alternatively, a seller may only accept credit cards and not money orders. That is fine.
- Note that this applies to online. If you work with someone in person and trust them, then electronic transfers are safer.

Rule #4

Investments, Social Security, & Medicare.

- Many people get fooled by commercials and phone calls that promise to get them extra benefits or cost savings.
- Never talk to anyone about your money who is not a Certified Financial Planner.
- Always verify their certification on www.cfp.net.
- CFPs are fiduciaries – They legally have to act in your best interest.
- Highly Recommended: Initially talk to someone at a well-known physical address and in person instead of over the phone.
- Your money and benefits are too important to leave to anyone else.
- A CFP can likely recommend other qualified people for things like Medicare.

Rule #5

Never Use Your Debit Card To Pay For Things

- Get several low-limit credit cards instead. For example, I have an airline card, a hotel card, and so forth, all with low limits.
- For websites that require you to store your credit card, you can use these different cards for different websites.
- Be sure to have the credit card app that allows you to “hold” or “freeze” your card should you have unauthorized transactions.
- Be sure to enable notifications for the credit card app so you’ll immediately see these notifications.

Rule #5.5

REPEAT: Never Use Your Debit Card To Pay For Things

- When fraud is detected with your debit card, your money has been taken out of your checking account. You have to work to get it back.
- Credit card companies are legally obligated to provide fraud protection. You are not responsible for someone committing credit card fraud with your card. They are. It is their money, not yours. You don't have to pay for fraud. You need to report it as soon as possible.
- If I carry a debit card, it is to get cash. I would take the debit card out of the safe, go inside my bank, use that ATM to get cash, then put the debit card back in the safe.

Rule #5.6

REPEAT, REPEAT: Never Use Your Debit Card To Pay For Things

- One attack against credit card companies dealt with the 3rd party payment processors used between the card terminal and the credit card company's systems.
- These attacks got credit card numbers as they were being processed.
- People using debit cards and running them like credit cards would have had their numbers stolen too.
- However, these stolen numbers would use the customer's checking account rather than the credit card company's account. No Fraud Protection! You would have to work with your bank to get your money back. Because it isn't their money, you may be looking at a long fight.

Rule #6
Keep a low amount of money in your checking account.

- Sometimes, you can be tricked into authorizing checking account withdrawals. It can be painful if you have a lot of money in there.
- Ask your bank to protect your savings accounts against electronic withdrawals. Ask your bank about any prohibitions on moving money from savings to checking regularly.
- Watch out for overdraft protection – you don't want a fake checking account withdrawal to pull from savings.
- Some banks have online savings accounts where you can move money around without penalty.

Rule #7

Think Passphrases, Not Passwords.

- When people think of passwords, they think of a single word, some numbers, and some special characters.
- Instead, think of multiple words. I grabbed two products from the medicine cabinet and combined some words. Here is what I came up with Ultra-Sheer-BLUE-EMU-SPF70. You can improve it by adding more special characters and numbers: Ultra-Sheer!BLUE-EMU^spf73012
- That was a quick and dirty method. Personally, I use dice and a word list from Diceware to generate secure passphrases.

Rule #8

Write down your passphrases and store them securely in your document safe.

- People used to say, “Never write down your passwords.” However, given today’s requirements for complexity, writing them down makes sense. However, you need to store them securely.
- If you have a safe at home, that may not be enough. Many safes are rated for fire – for example, 30 minutes at 1700F. They release moisture (i.e., steam) to keep the internal temperature safe. Steam isn’t good for documents. Use a smaller rated document safe inside your regular safe.
- Another tip: If you have computer materials (e.g., flash drives, DVDs), you’ll need a smaller rated safe for computer media as it has different requirements than documents.
- Never store passphrases or your passphrase “book” on a computer (e.g., Excel file). If you are hacked, you’ve given away the keys to your kingdom.

Rule #9

Be a liar on your security questions

- Security questions are used for account recovery. As we have seen, someone can use account recovery to take over your account. They do no good if your security questions can be found out easily (e.g., your mom's maiden name).
- Instead of answering the truth for these questions, invent an answer that has nothing to do with it. "What is your mom's maiden name?" Answer: "brass-lamp".
- Be sure to write the questions and answers down along with your passphrase.

Rule #10

Setup a username to login.

- If a website allows you to change your login to a username from an email address, you should do that. As we have seen, email addresses can be compromised.
- Your username shouldn’t be related to your name at all.
- As an example, a username could be AtlantisUnderWater.
- Each website should have a different username. Don’t reuse them. That defeats the purpose.
- Write down your username with your password, security questions, and the answers.

Rule #11

Use “Guest Checkout” rather than setup an account.

- If you go to a website rarely, maybe a couple of times a year, rather than set up an account, always use guest checkout if it is an option.
- Yep, it is an inconvenience to type your address in every time and your credit card, but if you only use that website a couple of times a year, what is the big deal?

Rule #12

If you have to setup an account, skip saving the credit card number (if it is allowed)

- Some websites require you to have an account to buy anything. However, when you enter your credit card information, they usually have a check box that says, “Save this card for future purchases.” Uncheck that box.
- Keep in mind that some website hacks get credit card information. Worse, they are routinely hacked because their security is terrible. I had to start using prepaid cards on one website because they continually got hacked.
- Yep, it is inconvenient to type your credit card, but what is the big deal if you only use that website a couple of times a year?

Rule #13

If you have to set up an account, use two-factor authentication.

- Two-factor authentication requires you to enter an additional code to log in. It is usually used if the computer/tablet/phone isn't recognized.
- After entering your password, you are prompted to enter a 6-digit code. Typically, this code is sent to your cell phone number. You would then enter this code in the prompt and log in normally.
- NEVER share this code with ANYONE.
- Advanced options include an authenticator application.

Rule #14

Set up login alerts for unknown locations

- If someone logs in from a device that has never been used before, you can be notified via email or text. If it wasn't you, your account has been compromised.

Rule #15

Set up notifications

- If you have an app for a credit card or something like that on your phone, you can enable notifications for specific events.
- For instance, I get notified on my phone if a credit card is charged more than $250.

Rule #15 - continued

Did you receive a notification that a hacker was able to access accounts, including passwords?

- Remember –don't believe emails or click on their links. Go to the app or directly to the website and check for information about the hacking incident there.
- If they were hacked, you'll want to change your password. Not once, Not twice, but three times.
- Why? Some websites allow account recovery if you know an old password. They usually keep the last one or two. Changing your password three times will flush out the old passwords.
- If you are on Facebook or other accounts with "Friends," and that account was hacked, go through your friends list and remove any people you don't know. Facebook has the option to recover your account through "Friends." A hacker may have added fake friends (fake accounts he controls) to take over your account again.
- Change the answers to your security questions.

Rule #16

Don’t use Facebook/Google/Amazon logins to access other websites.

- Some websites partner with Facebook, Google, or Amazon to allow you to log in to their websites using your username/password from Facebook, Google, or Amazon.
- While convenient, don’t do it.
- For example, if your Facebook account is compromised, a hacker can look at your “likes” and then try other websites to see if you were using your Facebook credentials to log in to them.
- The reason these companies do this is not for you. It is for them to track what you do when you are not on their platform. Your purchases are kept track of, and then they add that to their information about you.

Let's look at what an entry in our passbook would like (the one we store in the safe)

REI.com
Username: AtlantisUnderWater
Email: IamTheHappyCamper@yahoo.com
Passphrase: Ultra-Sheer!BLUE-EMU^spf73012
Security Questions

- What is my mom's maiden name: **brass-lamp**
- What was my first pet's name: **porkchop**
- What song was playing when you met your spouse: **her-dads-shotgun**

2 Factor Authentication to [phone number].
Login alerts enabled.
Notifications enabled (if applicable).

Preventative Measures

- Sometimes, the best method to not be scammed is not to see the scam emails or hear the scam callers. You can do this with filtering.
- The biggest downside is that filtering messages or phone calls may result in rejecting valid emails or callers.

Preventative Measures: Email

- There is an old saying: “You get what you pay for.” Many email clients are free and limited in what they can do.
- If you have a free email client and only communicate regularly with about 25 people or less, check if your email client can filter on your contact list. If it can, you can set up your email differently to better spot scammers.
- Create a contact list in your email client that includes each contact’s email address. Set up filtering so that any email from someone not on your contact list goes into a different email folder. You can name that folder “Unsolicited”

Preventative Measures: Email

- Your inbox will now consist of emails from people on your contact list. To see other emails, you must go to the folder “Unsolicited”
- The emails in “Unsolicited” you will treat very skeptically. If you see an email from someone in your contact list in the “Unsolicited” folder, it is likely because they used a different email address. That may be expected, or it may be because they were hacked.
- Some email clients already have something similar: it is “Focused” and “Other”

Preventative Measures: Email

- If security is important to you, you may want to consider paying for an email client to gain functionality.
- I've been working on Internet technologies since the days of dial-up. I will show you what I would do now if I had a clean slate.
- First, write down all your critical accounts. "Critical" means that you would struggle if they were hacked. Things like Facebook, PayPal, eBay, Amazon, and your financial accounts.

Preventative Measures: Email

- Some paid-for email clients allow you to have multiple email addresses (for example, 1 email address and 14 email aliases). This capability is extremely handy for security.
- I'll use a simple example. Say you have the following accounts: Amazon, Facebook, and Fisher-investments.
- Here is what I would create.

Preventative Measures: Email

- When you sign up for the first time, your username will be the default email account. You will never send this email address to anyone. You only use it to login to your email client.
- A newsletter email alias: This email is for newsletters and other offers where they ask you for an email address.
- A friends and family email alias: This email is intended for friends/family.
- A work/professional email alias: This email is for work/professional communication.
- An Amazon email alias: This would be the email for Amazon. Only Amazon knows it.
- A Facebook email alias: This would be the email for Facebook. Only FB knows it.
- A Fisher Investments email alias: This would be the email for Fisher-Investments.
- Non-critical accounts email alias: This would be the email for all other non-critical accounts.
- Do not make your critical accounts easy to guess. For example, your Amazon email is found and it has _Amazon at the end. A hacker can try _Facebook and see if that is your Facebook email.

Preventative Measures: Email

- You would then set up filtering, which can be very sophisticated. However, we only need to look at the destination email address to put the email in a folder. You would have an Amazon folder, a Facebook folder, a newsletter folder, and so forth.
- You have one email client, and one inbox, yet are very secure and can detect scams quickly. For instance, if you get Amazon “account problem” messages on your ‘newsletter’ email address, you know it is a scam. Amazon doesn’t have that email address!
- Please enable as much security on this email client as possible – complex passphrase, two-factor authentication, recovery codes, etc.

Preventative Measures: Landline Phone

- My mom has had the same phone number for over 50 years. Scammers know about it, but she doesn't want to change it cause of the hassle.
- We use a home phone product called the Vtech IS8251 which has smart call-blocking capability. There is much flexibility in this system. We use the toughest setting – allow list only.
- I put all my mom's friends, relatives, kids, grandkids, great grandkids on the allowed list. I also include the doctor's office, pharmacy, and sheriff's department (911). Anything not in the allow list gets blocked.
- Once a week, I go through the blocked calls to see if I recognize any numbers. However, all the family has my cell phone number, so they can call me and get on the allowed list!
- Now, when her home phone rings, it is always someone she wants to talk to.

Preventative Measures: Cell phone

- The same principle applies to a cell phone.
- Create a contact list of phone numbers and then choose “Do Not Disturb” except for contacts.
- Unsolicited calls get sent to voice mail.
- On an iPhone, you can use the Focus setting to prevent disturbances while driving or sleeping.
- Spend some time with family or a friend (and their cell phone) and set up Do Not Disturb exactly how you want.

Preventative Measures: Your Home Wi-Fi Network

- If you run a Wi-Fi network at home, you may want to greatly increase the strength of the pass-phrase, similar to what we do for our Internet accounts.
- Why? BadGuys with laptops and Wi-Fi antennas drive through residential areas and can access your Wi-Fi from across the street (or further). If you have a weak passphrase, they can join your network.
- Why do they do this? They may want to download child pornography, or perhaps they want to attack a government website or many other highly illegal activities.
- If law enforcement tracks down these illegal activities, they will think it is *someone in your household and not the Bad Guys*. Imagine if it was reported in the news that you were under investigation for downloading child pornography.

Preventative Measures: Your Home Wi-Fi Network

- No one wants to type a long password to join your Wi-Fi. Understood.
- Modern Wi-Fi devices have a WPS button on the Router or Access Point.
- WPS = Wi-Fi Protected Setup. It takes care of sharing your Wi-Fi password.
- Usually, you press and hold the WPS button on a router for a few seconds until the WPS light flashes.
- Then, on the device you want to use, stand next to the router and select WPS for that network.
- Wait a couple of minutes, and you should be good to go.

Preventative Measures: Contractors

- If any contractor makes you anxious or creates a sense of urgency, forget about them.
- Look for a Better Business Bureau rating, current license, current bond, and current references. Be sure to call those references.
- Don't be fooled by business cards with religious quotes on them. I've met some contractors that clearly weren't religious yet had business cards with great quotes from the Bible.
- Ask friends for references. Look for work done a while back so your friends have had a few months to evaluate the quality. Recognize that you may be better at spotting scammers than your friends – so references for recent work may not mean as much as you think.
- Be extremely wary if a natural disaster occurs. For example, if a hailstorm hit, many roofs may be damaged but not in danger of leaking. Work with your insurance company to ensure you can get your roof fixed maybe a year or two later when you are much less likely to run into a scammer and quality roofing contractors aren't overwhelmed with business.

Preventative Measures: Small Business

- A small business with an online presence must implement many things to keep it safe.
- However, if a hacker gets administrative access to the small business network, they can execute a ransomware attack on their data and all of their backups.
- One way to mitigate this attack is to use two backup drives. Each week, a drive is manually connected, a backup is run and stored on the drive, and then the drive is disconnected from the network and physically put in a safe.
- You would alternate between the drives week to week and keep the drives in a media-rated safe.
- Because the drives are only on the network for a limited time and are alternated weekly, you should have a relatively fresh copy of your data that the hacker cannot access.

Preventative Measures: Small Business

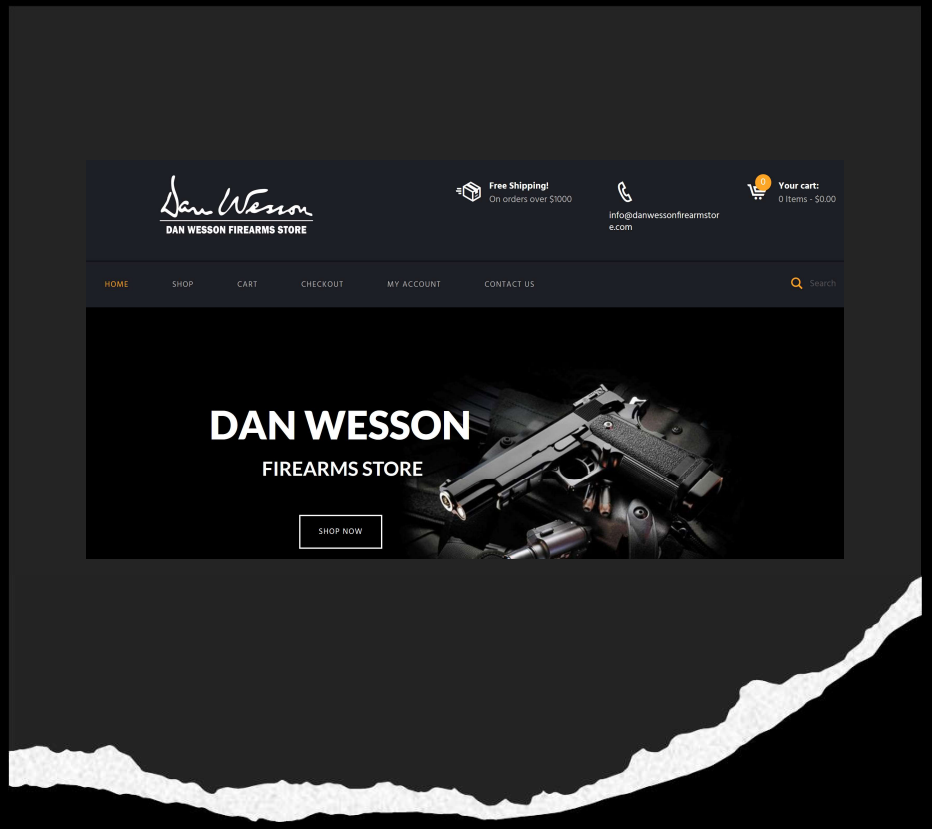
- If you were subject to a ransomware attack and have backup drives in the safe, do not put those drives on the network.
- You first must patch/fix how the hackers got in and remove any code that allows them to get back in.
- You should also report this crime.
- A StopRansomware guide is available: https://www.cisa.gov/sites/default/files/2023-06/stopransomware_guide_508c_0.pdf

Fake Website Example

- I like Dan Wesson 1911 pistols. I can never find them. So I search for “Dan Wesson Kodiak Buy”
- I see “danwessonfirearmstore.com” Sounds perfect.

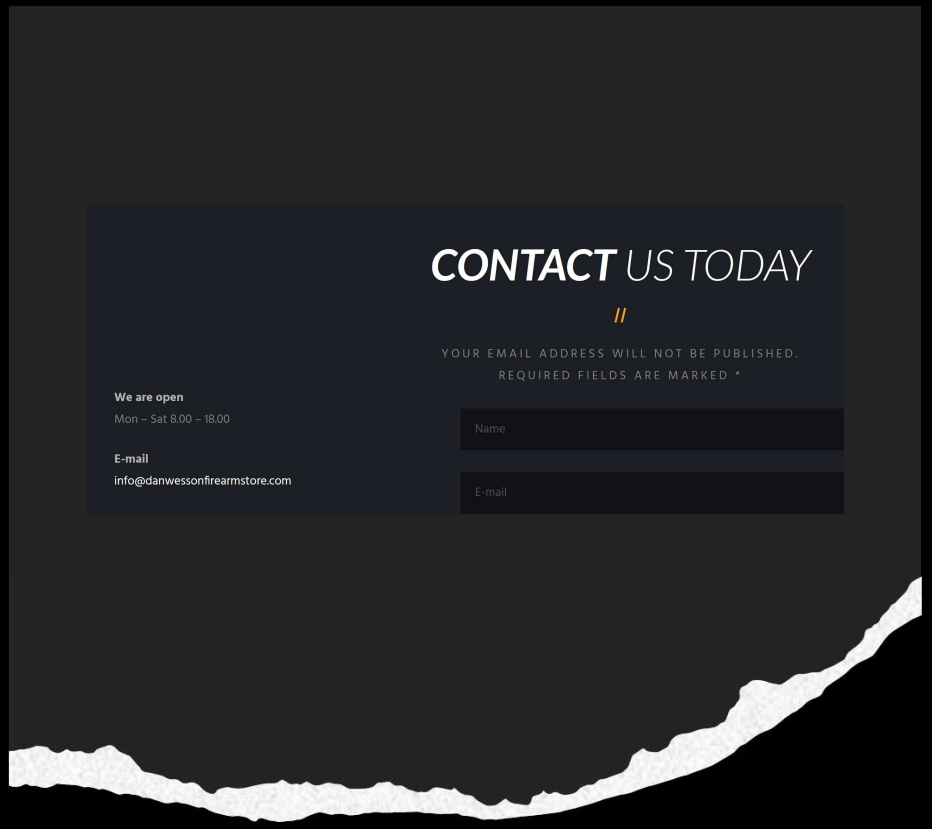
Fake Website Example

- A very professional-looking website.
- Let’s check “CONTACT US”



Fake Website Example

- They don’t list their FFL license number, nor do they list their authorized reseller number. Odd.
- They don’t have a street address. Odd.
- Their store hours are in military time. Odd.

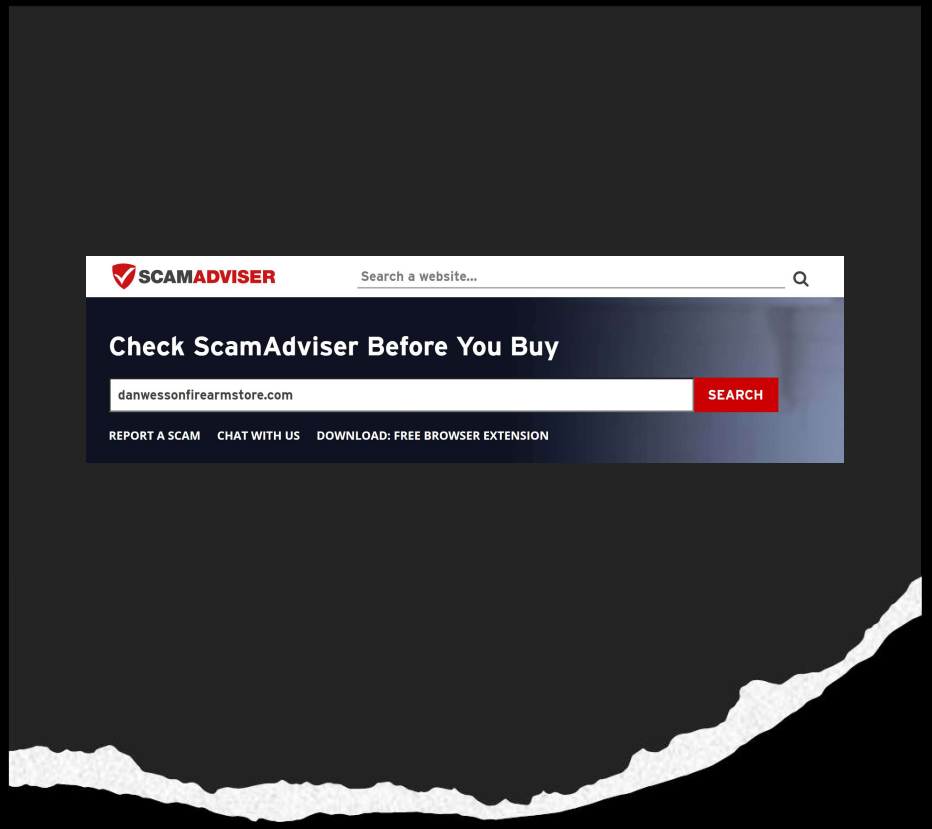


Let's check their website certificate

- Usually, certificates are issued for a year. This is for 3 months. Not a good sign.

Website checker

- Some websites have tools to check other websites.
- Let's check this store with https://www.scamadviser.com/



Website Checker Results

- Not looking good.

The positive

Positive highlights

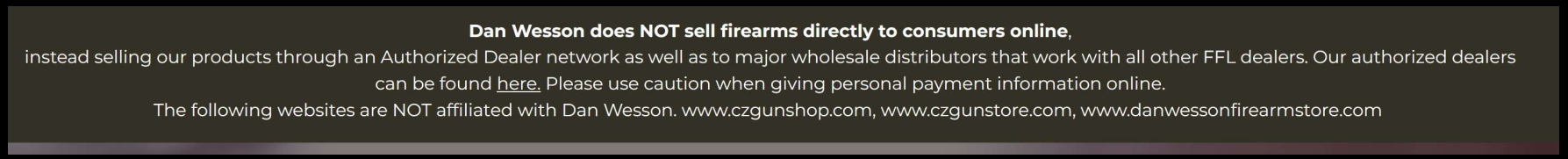
- Online shopping features were detected (**use our shopping scam checklist**)
- We found a valid SSL certificate
- The site has been set-up several years ago
- **DNSFilter** labels this site as safe
- Checked for malware and phishing by **Flashstart**

The negative

Negative highlights

- ✖ The identity of the owner of the website is hidden on WHOIS
- ✖ The Tranco rank (how much traffic) is rather low
- ✖ The server of the site has several low reviewed other websites
- ✖ The registrar of this website is popular amongst scammers
- ✖ **Cryptocurrency services** detected, these can be high risk
- ✖ Payment methods **support anonymous transactions** were found
- ✖ Negative reviews were detected for this website
- ✖ This website seems to be a gun store.

Let's check Dan Wesson's main site



- Not a good sign. I would get my firearm from an authorized dealer, not from this website.
- This website is an example that uses "scarcity" to scam users. When there is a rare item, such as the Dan Wesson Kodiak, they create a website and show the item "In Stock!"

What about a site we know is good?

- Let’s try my website: clayeolsen.com
- Looking better….

The good

- Some of the same things are listed here as they were on the bad website shown earlier.

The bad

- Since my website's URL is my name, I didn't think it was important to list my name on WHOIS.
- I'm not a bestselling author, so not much traffic.
- Remember to do your own checking in addition to this tool (like I did on the Dan Wesson store site).