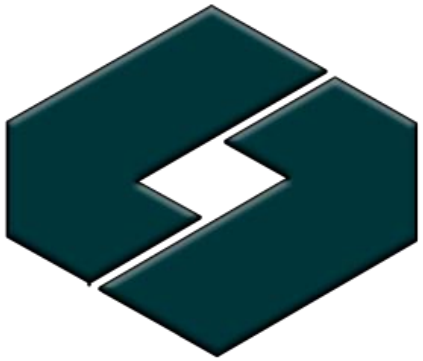


Backman Title Services

www.backmantitle.com

Data Security for Realtors (CORE)
RC251184

SB 165 (2024) – Title Recording Notice Requirements (Amends 17-21-6) – (Property Watch Everywhere)

Beginning Jan. 1, 2025, **requires County Recorders to create and maintain a system that allows a property owner to receive**, upon the property owner's election, **an electronic notice when the County Recorder records a deed or mortgage on the property owner's real property.**

- County Treasurer Tax Notice, for 2024, 2025 and 2026;
- Tax Notice must include a note and link that allows the property owner to elect/opt-in (must opt-in to receive electronic notice) top receive notice;
- Property Owner must provide an email contact.

Property Watch – Alerting you to recorded changes

Property Watch is a helpful service for homeowners in most Utah counties, keeping you updated on any recorded changes to your property. Enroll to receive email notifications whenever a document affecting your property's status is recorded. Available in the following Utah counties:

Salt Lake: https://slco.org/data-services/PropertyWatch/PropertyWatch.aspx
Utah: https://property-watch.utahcounty.gov/
Weber: https://www.webercountyutah.gov/forms/property_watch/
Davis: https://www.co.davis.ut.us/recorder/property-alert
Washington: https://www.washco.utah.gov/2021/11/04/sign-up-for-property-watch/
Cache: https://www.cachecounty.org/recorder/propertywatch/faq.html
Box Elder: https://erecord.boxeldercountyut.gov/eaglesoftware/eagleweb/fraudGuardSignup.jsp
Wasatch: https://kane.utah.gov/gov/dept/it/property-watch/
Duchesne: https://duchesne.utah.gov/
Uintah: https://co.uintah.ut.us:8443/ords/ucdev/r/property-watch-signup/home
Kane: https://kane.utah.gov/gov/dept/it/property-watch/
Beaver: https://www.beaver.utah.gov/123/Recorder
Grand: https://www.grandcountyutah.net/137/Recorder
Daggett: https://www.daggettcounty.org/CivicAlerts.aspx?AID=1324

Property Watch is on our utility lists!

Backman Title Services
www.backmantitle.com

Utility List - Salt Lake County

Primary Residence Status – Property Taxes

Notice: Utah law requires a property owner to declare the proper classification of their property whenever a deed records to obtain a primary residential tax exemption. Similar filings are also necessary to maintain or receive greenbelt property tax exemptions. Consult the county assessor's office to determine whether this exemption applies to this transaction.

Salt Lake County Assessor
https://slco.org/assessor/
2001 South State Street N2-600
Salt Lake City, UT 84114-7421
(385) 468-8000

Property Watch Service

Property Watch is a service available in your county. This service allows residents to stay in the loop about any recorded changes affecting their property. Once you enroll, you'll receive email notifications whenever a document is recorded that impacts your property's status.
https://slco.org/data-services/PropertyWatch/PropertyWatch.aspx

Backman Title Services
www.backmantitle.com

Owner's Policy Comparison*

	Coverage	ALTA basic	ALTA Extended Owner's	ALTA Home owner's
1	Someone else owns an interest in your title	X	X	X
2	A document is not properly signed	X	X	X
3	Forgery, Fraud, Duress	X	X	X
4	Defective recording of any document	X	X	X
5	There are restrictive covenants	X	X	X
6	There is a lien on your title because there is: a) a deed of trust, b) a judgment tax of special assessment, c) a charge by the Homeowners Association	X	X	X
7	Title is unmarketable	X	X	X
8	Mechanic's lien protection		X	X
9	Unrecorded liens by a homeowner's association		X	X
10	Unrecorded easements		X	X
11	Rights under unrecorded leases, contracts, or options		X	X
12	Forced removal of a structure because it: a) extends onto other land or onto an easement, b) violates a restriction in schedule B, c) violates existing zoning law*			X
13	Can't use land for SFD because the use violates a restriction in schedule B or Zoning			X
14	Pays rent for substitute land or facilities			X
15	Plain Language			X
16	Building permit violations*			X
17	Compliance with Subdivision Map Act*			X
18	Restrictive covenant violations			X
19	Post Policy forgery			X
20	Post Policy encroachment			X
21	Post Policy damage from mineral/water extraction			X
22	Post Policy living trust coverage			X
23	Enhanced Access- Vehicular & Pedestrian			X
24	Map not consistent with legal description			X
25	Post Policy automatic increase in value up to 150%			X
26	Post Policy adverse possession			X
27	Post Policy cloud on title			X
28	Post Policy prescriptive easement resulting in reversion			X
29	Covenant violation resulting in reversion			X
30	Boundary walls and fence encroachment*			X
31	Enhanced marketability			X
32	Violations of building setbacks			X
33	Discriminatory covenants			X
34	Insurance coverage forever			X

*Subject to a deductible

Corporate Phone (801) 288-8818
Layton Phone (801) 774-8818
Midvale Phone (801) 263-1500
Riverwoods Phone (801) 224-9020
Salt Lake Phone (801) 433-0506
Bountiful Phone (801) 295-7676
Farmington Phone (801) 683-4440
Ogden Phone (801) 475-6100
Lehi Phone (385) 336-8390
St. George Phone (435) 688-8808

	Coverage	ALTA basic	ALTA Extended Owner's	ALTA Home-owner's
1	Someone else owns an interest in your title	X	X	X
2	A document is not properly signed	X	X	X
3	Forgery, Fraud, Duress	X	X	X
4	Defective recording of any document	X	X	X
5	There are restrictive covenants	X	X	X
6	There is a lien on your title because there is: a) a deed of trust, b) a judgment tax of special assessment, c) a charge by the Homeowners Association	X	X	X
7	Title is unmarketable	X	X	X
8	Mechanic's lien protection		X	X
9	Unrecorded liens by a homeowner's association		X	X
10	Unrecorded easements		X	X
11	Rights under unrecorded leases, contracts, or options		X	X
12	Forced removal of a structure because it: a) extends onto other land or onto an easement, b) violates a restriction in schedule B, c) violates existing zoning law*			X
13	Can't use land for SFD because the use violates a restriction in schedule B or Zoning			X
14	Pays rent for substitute land or facilities			X

		ALTA basic	ALTA Extended Owner's	ALTA Home-owner's
15	Plain Language			X
16	Building permit violations*			X
17	Compliance with Subdivision Map Act*			X
18	Restrictive covenant violations			X
19	Post Policy forgery			X
20	Post Policy encroachment			X
21	Post Policy damage from mineral/water extraction			X
22	Post Policy living trust coverage			X
23	Enhanced Access- Vehicular & Pedestrian			X
24	Map not consistent with legal description			X
25	Post Policy automatic increase in value up to 150%			X
26	Post Policy adverse possession			X
27	Post Policy cloud on title			X
28	Post Policy prescriptive easement resulting in reversion			X
29	Covenant violation resulting in reversion			X
30	Boundary walls and fence encroachment*			X
31	Enhanced marketability			X
32	Violations of building setbacks			X
33	Discriminatory covenants			X
34	Insurance coverage forever			X

Corporate Identity Theft Notification

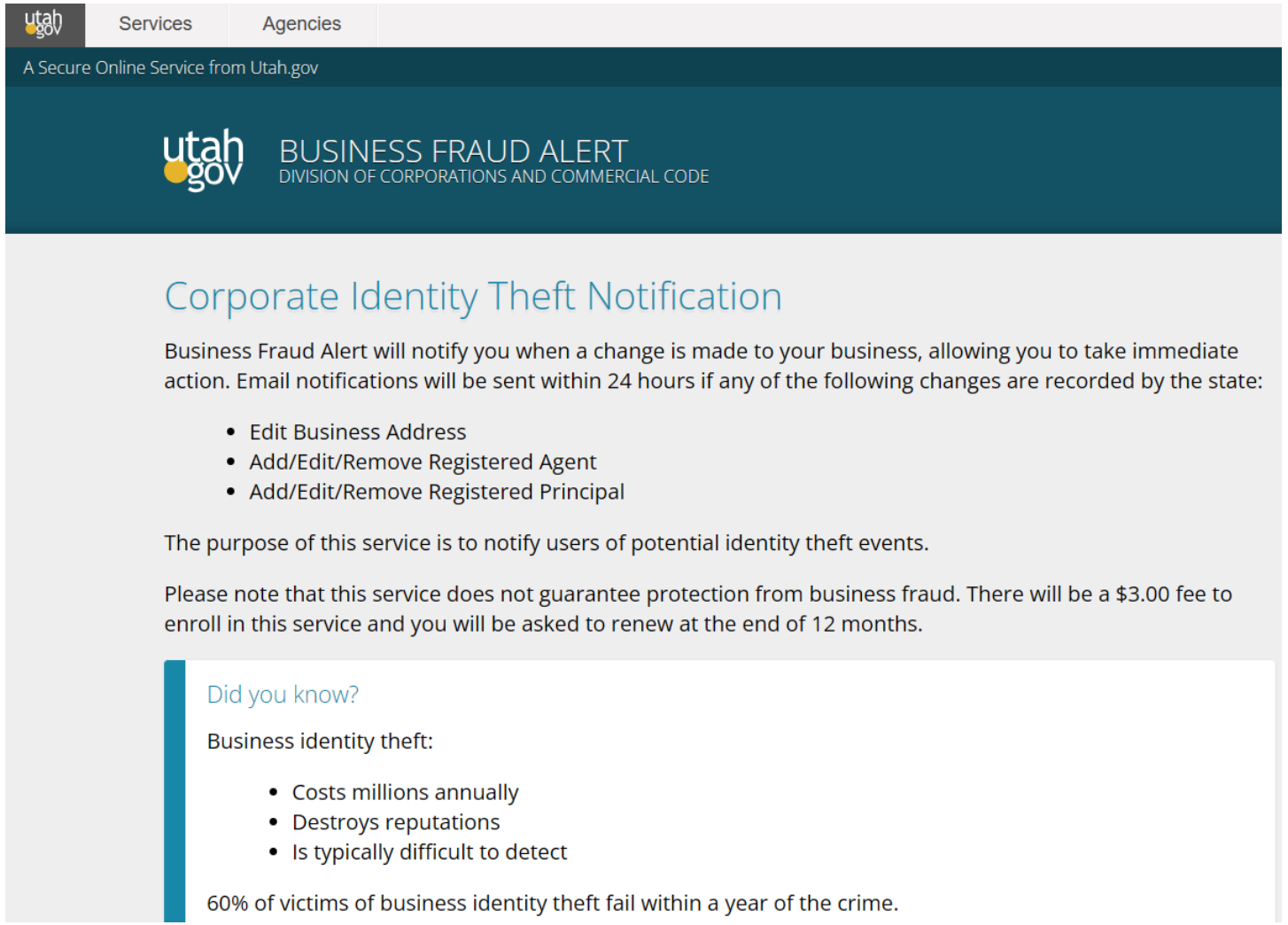
Business Fraud Alert will notify you when a change is made to your business, allowing you to take immediate action. Email notifications will be sent within 24 hours if any of the following changes are recorded by the state:

- Edit Business Address
- Add/Edit/Remove Registered Agent
- Add/Edit/Remove Registered Principal

The purpose of this service is to notify users of potential identity theft events.

- Please note that this service does not guarantee protection from business fraud. There will be a $3.00 fee to enroll in this service and you will be asked to renew at the end of 12 months.

https://secure.utah.gov/fraudalert/



Cor te Identity Theft Noti tion

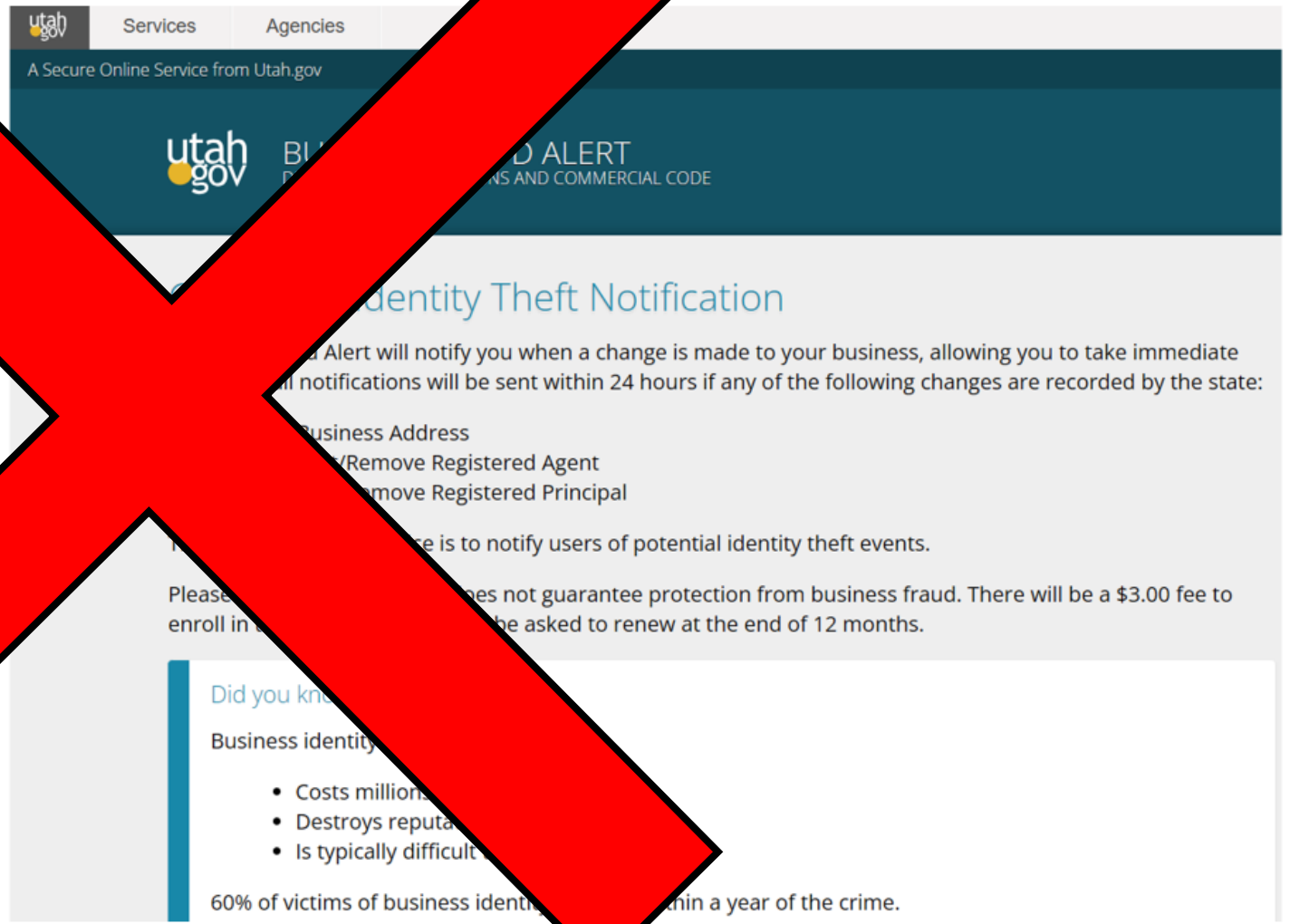
Business Fraud Alert will notify y
change is made to your busine
you to take immediate action. En
notifications will be sent within 24 h
any of the following changes are reco
by the state:

- Edit Business Address
- Add/Edit/Remove Registered Agent
- Add/Edit/Remove Registered Principal

The purpose of this service is to notify users
of potential identity theft events.

- Please note that this service does n
guarantee protection from busi
There will be a $3.00 fee to en
service and you will be ask w at
the end of 12 months.

https://secure.utah.gov/fraud



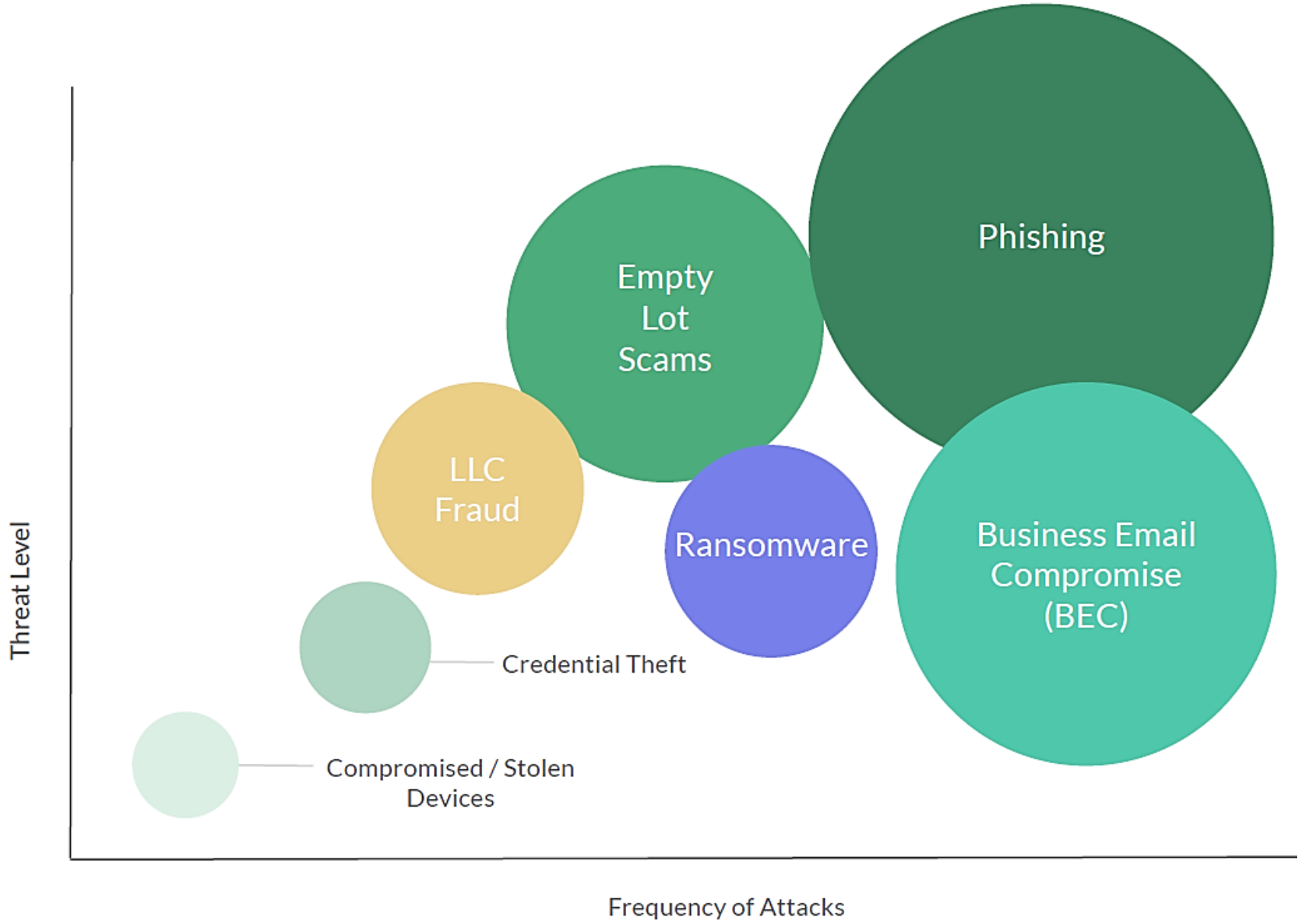
Security Review

- Security Best Practices
    1. Phone
    2. Laptop
    3. Tablet
- Passwords
- MFA (Multi-Factor Authentication)
- Vulnerabilities
- Ways to Protect Your Business

Multiple Fraud Methods used to Hijack a Transaction

- Fraud is becoming more complex and multi-layered, therefore requires a multi-pronged approach to prevent it

- Responses to a survey of the frequency and types of attacks businesses suffered in the last 12 months



Backman

Title Services

CYBER CRIME

Client email 1 – Bennion Closing (7:07 am)

Closing: **Correct Property Address**

EO

EO Name & Fake Email backmanstitle.com>

To **Buyer**

Cc **Realtor Name, & Fake email & Lender Name Fake email**

Reply | Reply All | Forward

Day 2023 7:07 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Hello **Buyer's Last Name**

Can you please confirm whether it will be possible to wire the closing funds to the title account today? If so, I will send you the wiring instructions for your reference. All of the closing files are ready in advance of a smooth closure and disbursement of funds .

Thank you,

EO Name

Our EO's exact email Signature

Backman
Title Services

Closing: **Correct Property Address**

EO

EO Name & Fake Email backmanstitle.com>

To **Buyer**

Cc **Realtor Name, & Fake email & Lender Name Fake email**

Reply | Reply All | Forward

Day 2023 7:07 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Hello **Buyer's Last Name**

Can you please confirm whether it will be possible to wire the closing funds to the title account today? If so, I will send you the wiring instructions for your reference. All of the closing files are ready in advance of a smooth closure and disbursement of funds .

Thank you,

EO Name

Our EO's exact email Signature

Backman
Title Services

Clever Fraudster!

Sender: username@backmanstitle.com

Realtor: username@Sanchezere.com

Lender: username@diamondsmortgage.com

Client email 2 – Bennion Closing (7:12 am)

Re: Closing: **Correct Property Address**

FR

Realtor Name, & fake email
To **EO Name with fake email**
Cc **Client Name/email & lender name & Fake email**

Reply | Reply All | Forward

Day 2023 7:12 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Good morning!

Thanks **EO** As required, **Buyer** advise if it will be possible to start remitting the closing funds to the escrow account today so funds can disperse early.

Thanks!
Realtor Name

Client email 3 – Bennion Closing

On ' **Same Day** **Bennion** **Bennion email** @gmail.com> wrote:

> Yes let's go ahead! Let us know what we need to do. Thank you!

Client email 4 – Bennion Closing (8:24 am)

Re: Closing **Correct Property Address**

EO **EO Fake email** @backmanstitle.com>

To **Buyer Name**

Cc **Realtor name & Fake email & lender name & Fake email**

Reply | Reply All | Forward

Day 2023 8:24 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

WIRING INSTRUCTIONS.pdf
.pdf File

Hello **Client's Last Name**

Please find attached herein the closing instructions to wire the funds at your bank. The final amount to be remitted is $45,106.48. Kindly send me a confirmation email once the funds are processed today before the wiring cut off time.

Thank you,

EO name

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
image.png

Our EO's exact email Signature

Fake Wire Instructions

Backman Title Services

(Midtown Office)
1441 E 41st Street
#110
Tulsa, OK 74105

(Corporate Office)
10129 S Yale Avenue
Tulsa, OK 74137
(918) 392-9700 Main Phone

(Owasso Office)
9500 N 129th E Avenue, Suite
Owasso, OK 74055

Our Utah
Office Address

WIRING INSTRUCTIONS

Metropolitan Commercial Bank
99 Park Ave
New York, NY 10016

ABA: 026013356

For Credit to the Account of: **Brendan Backman Escrow Services**

Our Utah Office Address

Account Number: 253255749782

Please Reference the Following: 111605-006040

Important Notice: "We will **NOT** be able to accept "ACH" Transactions....
It must be a wire transfer.

Client email 5 – from Bennion (10:07 am)

(Subject: We were almost scammed by wire fraud)

From: **Buyer Name & email**
Sent: **Day** 10:07 AM
To: **Correct names & emails of Escrow officer, Realtor & Loan officer**
Subject: We were almost scammed by wire fraud

⚠ **EXTERNAL EMAIL:** Open links/attachments cautiously.

Hey everyone,

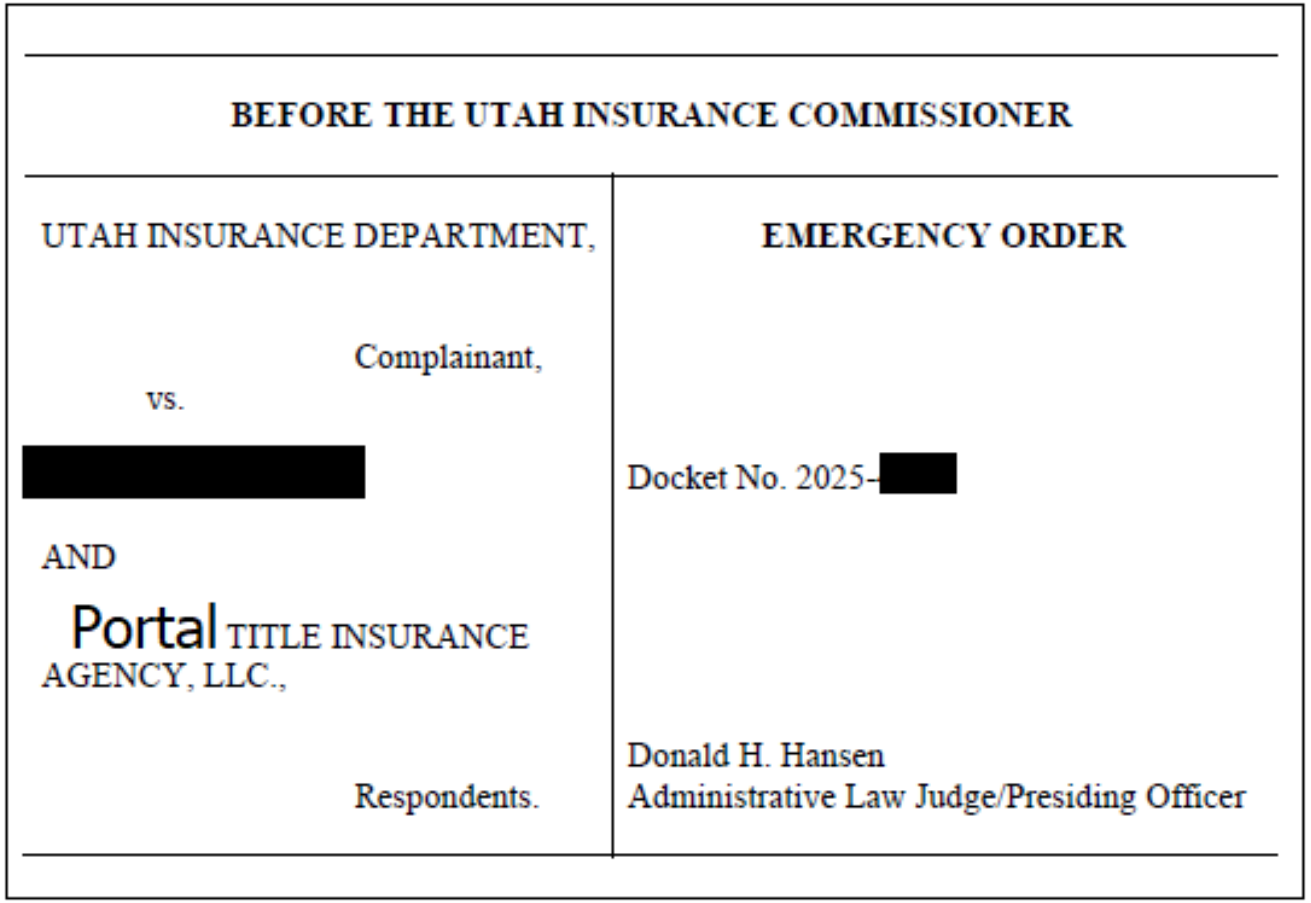
If you haven't heard the news from us or **Agent** :ext/call yet, just wanted to let you know we were almost scammed by a wire fraud attempt. The scammers obtained our email history and asked us to wire $46,000 today, with instructions in an attacned par. Everything looked really legit, but the sender addresses were spoofed and different by one letter (backmanstitle instead of backmantitle, **lender** :mortgage etc). We initiated a wire transfer through our bank but luckily caught it right away so I was able to call **CU &** cancel it. If you have any emails from the red underlined addresses below please report them as Phishing/scam.

Everyone should change their email password asap and log out of all unused devices. I'll be doing that as well.


Whew!

The EMERGENCY Order

- The Utah Insurance Department issued an Emergency Order
- The UID received Notice from First American Title that they had terminated their Agency Agreement with Portal Title
- FATCO had been informed that Portal Title had “closed its doors”
- FATCO was informed that Portal Title is dissolving



BEFORE THE UTAH INSURANCE COMMISSIONER

UTAH INSURANCE DEPARTMENT, Complainant, vs. [redacted] AND Portal TITLE INSURANCE AGENCY, LLC., Respondents.	**EMERGENCY ORDER** Docket No. 2025-[redacted] Donald H. Hansen Administrative Law Judge/Presiding Officer

d. [redacted] further indicated to First American that she is dissolving the company. [redacted] stated that she had a "wire fraud incident" in October 2024 and was going to file personal bankruptcy to get out of an office lease with [redacted]

- Portal Title had a "wire fraud incident" and the owner is filing personal bankruptcy
- Multiple Consumer Complaints began to be filed regarding Escrow Funds on Deposit with Portal Title

f. On April 15, 2025, the Department contacted the Respondents by both phone and email. The Department notified the Respondents of the consumer complaint and ordered the Respondents to provide information to the Department regarding the consumer escrow transaction.

g. On April 16, 2025, the consumer contacted the Department stating that the consumer still had not been contacted by the Respondents and that the escrow issue had not been resolved. The consumer further advised the Department that he had spoken to former escrow agents with [redacted] who indicated that other clients of the Respondents had also not received their escrow money held on deposit with [redacted] and that the money was no longer in the Respondents' account.

h. On April 16, 2025, the Department again contacted the Respondents via email, through [redacted] regarding the new information received from the consumer. [redacted] was ordered to provide an immediate response to the Department. Respondents failed to respond.

i. [redacted] does not have affiliation/appointment with a title insurer as described in Section 31A-23a-115.

in touch with anyone at [redacted] nor had he received any contact from the Respondents regarding the release of his escrow funds. The consumer further advised that he had approximately $7,000 of escrow monies on deposit with [redacted]

g. On April 16, 2025, the consumer contacted the Department stating that the consumer still had not been contacted by the Respondents and that the escrow issue had not been resolved. The consumer further advised the Department that he had spoken to former escrow agents with [redacted] who indicated that other clients of the Respondents had also not received their escrow money held on deposit with [redacted] and that the money was no longer in the Respondents' account.

h. On April 16, 2025, the Department again contacted the Respondents via email, through [redacted] regarding the new information received from the consumer. [redacted] was ordered to provide an immediate response to the Department. Respondents failed to respond.

How is a Closing Protection Letter (CPL) different from an owner's or lender's title insurance policy?

The lender's policy is issued as a guarantee of borrower covenants and insures the lenders desired lien position. The policy is mainly provided to insure against defects and liens from the past. A lenders policy is only issued after a loan has funded and recorded and the effective date is based on when the deed of trust is recorded.

A CPL gives the insured extra coverage for events that may happen before, during and after settlement. While protection for the lender's begins after the securing document is recorded, coverage from the CPL becomes effective upon the delivery of the title commitment.

A CPL is also different because the underwriter insures the lender against actions of their title agency. A lenders requests a CPL because the actions of a title agency prior to the issuing of the policy can affect the ability to enforce a lien. It is also true that some agency actions can also put a lenders funds at risk.

When the CPL is issued the underwriter backs up actions made by an individual title agent. Among other things, and subject to certain exclusions, the underwriter guarantees their title agent will not:

1- Fail to comply with a lender's written closing instructions
2- Fail to properly record documents
3- Act in a negligent or fraudulent way

About Closing Protection Letters

1- The entire Closing Protection Letter fee is be remitted directly to the underwriter
2- The CPL fee is only be charged if a transaction closes
3- The CPL fee appears on both the ALTA Settlement Statement and lender Closing Disclosure as a charge to the borrower.

The Dangers of QR Codes

QR Codes – Masters of Disguise

Make it impossible to see where the link is going BEFORE actually visiting the site

QR Codes are EASY to generate

QR Codes are Easily Replaced – both on electronic communications and in physical locations


Private (free) vs.
Corporate/Enterprise email

Free email providers

AOL Mail

Microsoft® Hotmail®

Scary Statistics (PWs)

- One criminal group averaged between 5 and 10 million email authentication attempts daily and success with anywhere from 50,000 to 100,000 working inbox credentials.
- Microsoft reported 1 in every 250 **corporate accounts** is compromised every month (last year they had 240 million active users)
- There are hundreds of password “dumps” with billions of stolen passwords.

Password Management

- Passwords have always been linked to a high degree of cyber risk exposure.
- Weak and Unsecured passwords are the SINGLE BIGGEST reason for DATA BREACHES.

- https://youtu.be/opRMrEfAIiI

How are Hackers getting Passwords?

- Brute-Force - most passwords made up by people are guessable within hours or days (if not instantly)
- Data Breaches of sites/services you use – this information is often compiled into data bases and sold or shared freely
- Credential Stuffing – use of automated bots to try every username/password combination from another website until one of them works
- Password Spraying – using a list of the most used passwords until they gain access
- Phishing/Smishing – tricking someone into entering logging information into a phony login screen
- Social Engineering – Pretending to be someone they're not through texts, emails, or phone calls to get you to give them information
- Keylogging Viruses – getting you to click on a link in a malicious email that installs malware that logs your keystrokes

Data Breaches - https://en.wikipedia.org/wiki/List_of_data_breaches

- Yahoo - 2018, 2014
- LinkedIn – 2021
- Facebook – 2019
- Marriot International – 2018
- MySpace – 2013
- Adobe – 2013
- AOL – 2004, 2006, 2014
- MyFitnessPal

';--have i been pwned?

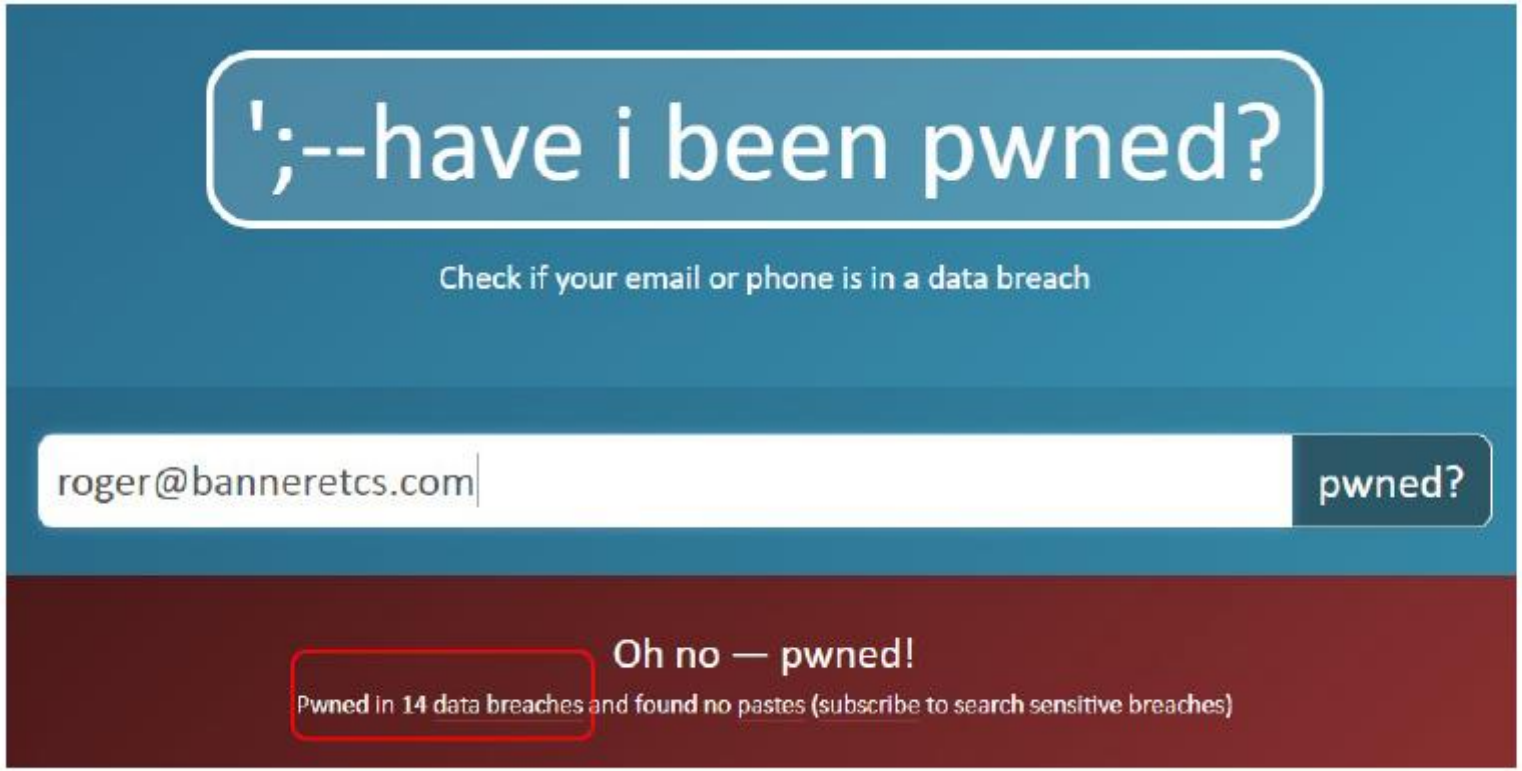
Check if your email address is in a data breach

thodgson@backmantitle.com pwned?

Oh no — pwned!

Pwned in 7 data breaches and found no pastes (subscribe to search sensitive breaches)

https://haveibeenpwned.com/



Password Compromises Include:

- Facebook.com
- Twitter.com
- Diet.com
- Mgm.com
- Citibank.com
- Experian.com
- Govconnect.com
- My healthcare provider

https://haveibeenpwned.com/

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

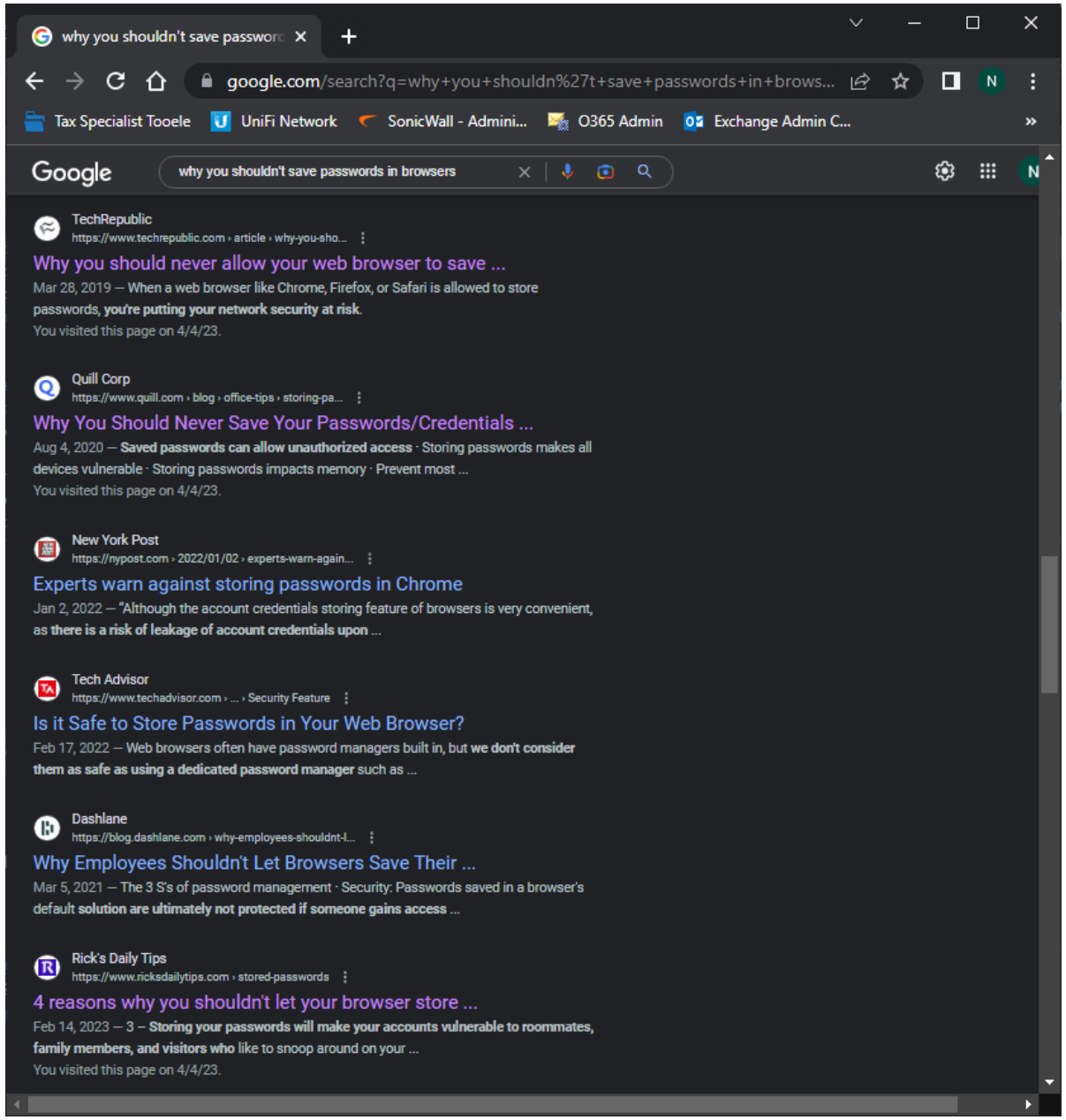
Compromised data: Email addresses, IP addresses, Passwords, Usernames

How Secure are my Passwords Stored in my Browsers?

- Web Browsers ARE NOT password managers
- Web Browsers are easy to break into, and lots of malware, browser extensions and even honest software can extract sensitive information from them
- Using malware, hackers can EASILY gain access to your ENTIRE LIBRARY of passwords across ALL websites you visit. Your exposure footprint is MASSIVE.
- Ransomware could force encrypt browser-stored passwords and block access to ALL your websites/services
- Device sharing is commonplace among the Work From Home culture potentially leaving us vulnerable and non-compliant
- Any encryption is worthless since the key to the encryption is easily locatable in an unprotected configuration file

How Secure are my Passwords if they are Stored in my Browsers?

https://youtu.be/Vlble8_TKS4



Biggest Password Problems and Risks Today

- The average person logs on to 170+ sites/services but only uses between uses 3 and 19 passwords
- Weak Passwords
  - 10 Characters or less
  - Predictable Complexity
    - i.e.: (1234 / 2023! / Seasons / Names of Places / People / House Numbers / Street Names / Birthdays / Birth Years)
- Shared Passwords/Password Patterns between multiple sites/services
- Passwords that are easy for adversaries to guess
- One compromise more easily leads to other compromises

PASSWORD COMPLEXITY

Top 30 Most Used Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

Number of Characters	Numbers Only	Lowercase Only	Uppercase & Lowercase	Numbers, Uppercase & Lowercase	Numbers, Uppercase, Lowercase, & Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 seconds	7 seconds	31 seconds
8	Instantly	Instantly	2 minutes	7 minutes	39 minutes
9	Instantly	10 seconds	1 hour	7 hours	2 days
10	Instantly	4 minutes	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 seconds	2 days	24 years	200 years	3,000 years
13	19 seconds	2 months	1,000 years	12k years	202k years
14	3 minutes	4 years	64k years	750k years	16 million years
15	32 minutes	100 years	3 million yrs	46 million yrs	1 billion years
16	5 hours	3,000 years	173 million yrs	3 billion yrs	92 billion years
17	2 days	69k years	9 billion yrs	179 billion yrs	7 trillion
18	3 weeks	2 million yrs	467 billion yrs	11 trillion yrs	438 trillion years

Passwords

- The length of your password is far more important than complexity –
  18 Characters (Minimum)
- Use a Passphrase instead of a Password
- Unique - DO NOT re-use passwords across multiple systems/websites
- Use KeePass to autogenerate and store passwords (instructions emailed 5/17/2023)
- DO NOT use browser stored passwords

PASSWORD BEST PRACTICES

- ***NEVER allow your browser to remember your username and password – this is an egregious security vulnerability***
- DO NOT re-use passwords for your work email anywhere else for any other website/service
- DO NOT co-mingle passwords between personal accounts and work accounts
- ALWAYS use original passwords for work accounts
- DO NOT re-use passwords between websites / services that you use for work – each account you use should have its own original username and its own original password that is not used anywhere else for any other account – password managers create random passwords, no creativity required!
- Use a password manager to manage your usernames and passwords
- DO NOT use the Browser's Password Auto-Save Feature to remember your passwords – **IT IS NOT SECURE**
- DO NOT leave passwords for shared computers in Public Places on Post-It notes, white boards, or taped to the bottom of keyboards

Are Your Passwords in the Green?

Number of Characters	Numbers Only	Lowercase Only	Uppercase & Lowercase	Numbers, Uppercase & Lowercase	Numbers, Uppercase, Lowercase, & Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 seconds	7 seconds	31 seconds
8	Instantly	Instantly	2 minutes	7 minutes	39 minutes
9	Instantly	10 seconds	1 hour	7 hours	2 days
10	Instantly	4 minutes	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 seconds	2 days	24 years	200 years	3,000 years
13	19 seconds	2 months	1,000 years	12k years	202k years
14	3 minutes	4 years	64k years	750k years	16 million years
15	32 minutes	100 years	3 million yrs	46 million yrs	1 billion years
16	5 hours	3,000 years	173 million yrs	3 billion yrs	92 billion years
17	2 days	69k years	9 billion yrs	179 billion yrs	7 trillion
18	3 weeks	2 million yrs	467 billion yrs	11 trillion yrs	438 trillion years

Multi-Factor Authentication

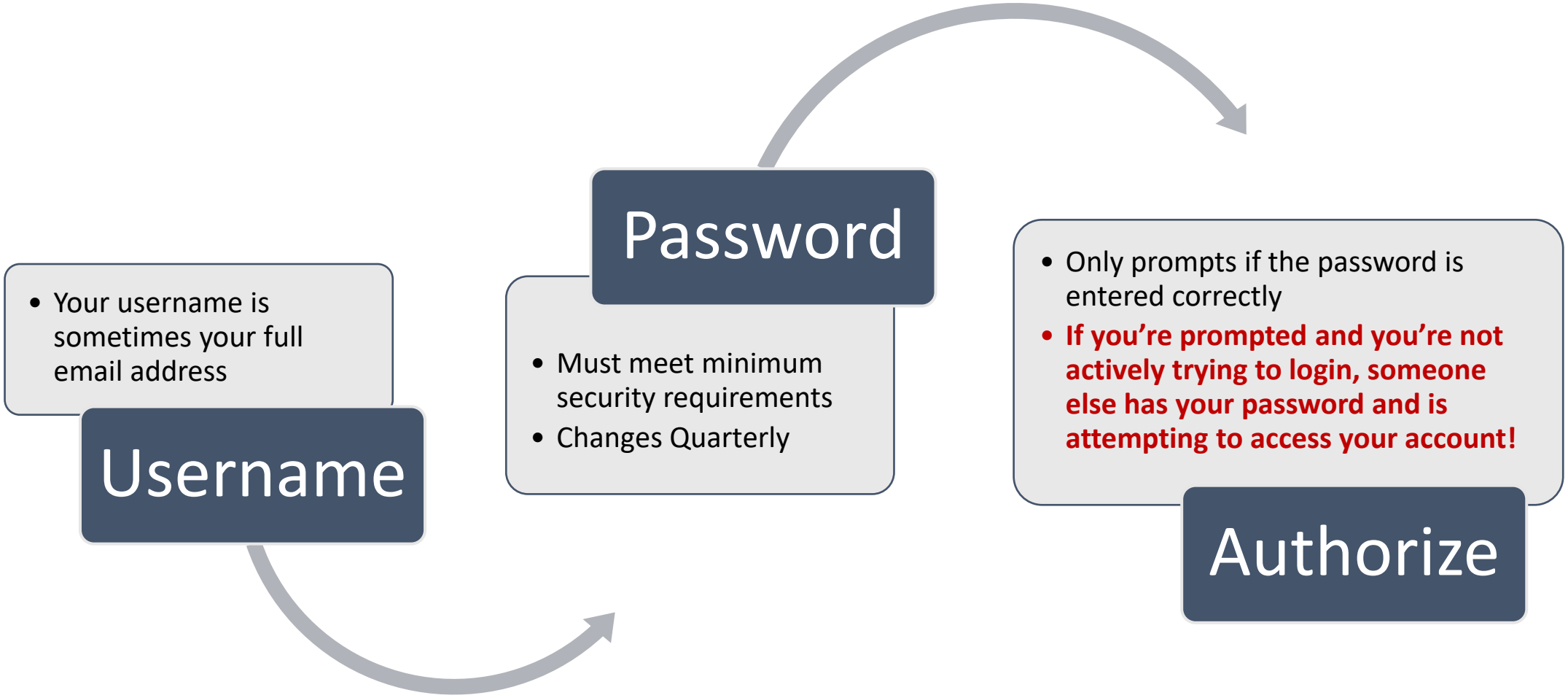
What is it and why is it important?

Systems that require the user to provide two or more verification factors to gain access to a resource. Usernames & passwords are vulnerable to brute force attacks and can be stolen

3 Most common methods

1. Multi-Factor includes something you know (a password or PIN)
2. Something you have (an app on your phone, or another type of key)
3. Something you are (biometrics like fingerprint or facial recognition). Enable MFA on accounts whenever possible.

Multi-Factor Authentication



What's the Difference?

Spoofed

- Spoofers forge signature block information & can cloak the reply address
- Spoofers do not gain access to your email account of the information in it
- There is no way to prevent spoofing ☹
- Never tell anyone you've been "Hacked"

Hacked

- If hackers gain control of your device/email account, what can you do?
  1. Act!
  2. Change your Password
  3. Change Security Answers
  4. Enroll in MFA
  5. Review email account settings
  6. Run a Virus Scan

What can you do?

You are the crucial piece of the puzzle to keeping your data safe!

- Training
- Strong Passwords
- Anti-virus
- Multi-Factor Authentication
- Software Updates

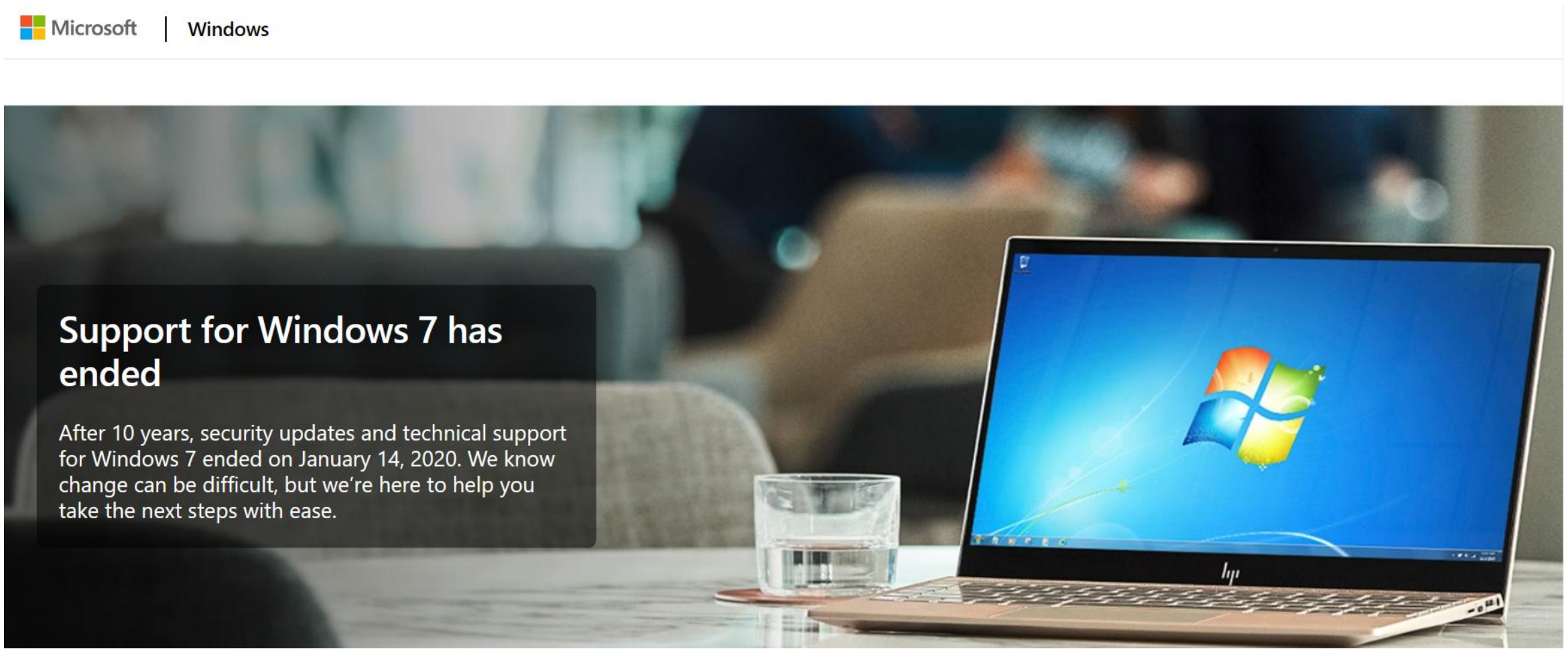
Operating Systems & Security Updates

Microsoft | Windows

What does Windows 8.1 end of support mean for you?

Change can be difficult, but we're here to help you take the next steps. As of January 10, 2023, Microsoft no longer provides security updates or technical support for Windows 8.1. You might be able to upgrade your Windows 8.1 device to a newer version of Windows, but we recommend moving to a new PC that can run Windows 11 as the best option.

Operating Systems & Security Updates



Operating Systems & Security Updates

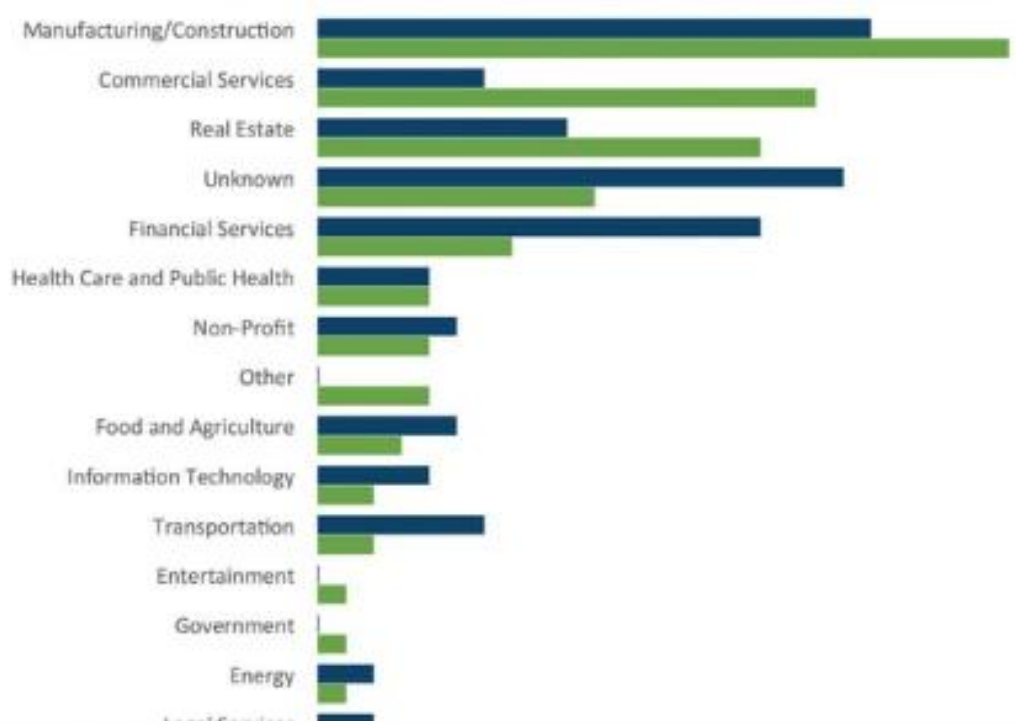
Microsoft | Windows

Support for Windows 10 will end in October 2025

After October 14, 2025, Microsoft will no longer provide free software updates from Windows Update, technical assistance, or security fixes for Windows 10. Your PC will still work, but we recommend moving to Windows 11. Windows 11 offers a modern and efficient experience designed to meet current demands for heightened security.

Business Email Compromise Losses Are the Highest Type by Amount

Real Estate is the 3rd Highest Targeted Industry



By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Scary Statistics (BEC) - 2022

Attacks have increased by 81% in the last year

98% of employees failed to report the threats

15% of employees respond to malicious content

21,832 BEC Complaints

Estimated losses totaling more than $2.7 billion dollars

ALL IT TAKES IS ONE CLICK - Don't Do it!

Email viruses are often connected with phishing attacks, in which hackers send out malicious messages that look as if they are originated from legitimate, known or trusted sources, such as the following:

•Financial institutions;

•Real Estate Agents or Agencies;

•Title Companies;

•Friends, relatives or co-workers; or

•Someone high up in the company

- **When you receive a malicious email, IT IS NOT necessary for you to enter login information for you to be compromised. ALL IT TAKES IS A SINGLE CLICK, and the damage has already been done.**
- **Here are the things clicking on a link/attachment can do to our system:**
  - **Distribute & Execute a Ransomware Attack**
  - **Unleash a Keylogger Virus**
  - **Password Harvester Virus**
  - **Provides Bad Actors Invisible Remote Access to Your Computer & Back Door Access to your Files**
  - **Harvests Data and Destroys Files**

REMEMBER: A hacker only must be lucky once, but you must be right 100% of the time

Time Flies When You're Getting Hacked

It takes an average of 212 days for organizations to discover a data breach – that's a long time compared to the 24 to 48 hours it takes for a hacker to compromise the domain admin once they've gained initial access to your system.

Requirements for use of Personal Devices

Current / Supported operating system

- Windows 11
- Windows 10 support ends October 14, 2025;
  Windows 8.1 support ended January 10, 2023;
  Windows 7 support ended January 14, 2020

Subscribe to an Anti-Virus Software

- Virus Definitions must be kept up to date
- *Scheduled* scans must run at least once weekly – scanning daily is better!

Requirements for use of Personal Devices

Smartphones/Tablets

- Secure your device with a PIN or Biometric Security
- Turn on your device's Auto-Lock feature and always lock it when not in use
- Install a Trusted Security App (Norton/McAfee/etc.)
- Be cautious when installing & setting up apps – use trusted sources such as Google Play Store and Apple App Store and make sure Apps only have access to systems on your phone they require to function
- Install Operating System Updates when available
- Avoid using public/unsecured Wi-Fi networks when possible
- Turn off Blue Tooth/Wi-Fi when not in use to prevent others from connecting to your device
- Beware of Suspicious emails, text messages, and links that can infect your device
- Turn off location tracking services when not in active use

Don’t Let the Vampires In!

- Be careful about opening attachments from unknown sources.
- Avoid opening files included as attachments.
- Never click on links in the body of email messages from unknown sources.
- Double-check the sender's name to confirm that an email is from a legitimate source.
- Watch for red flags that may indicate phishing emails, such as obvious grammatical errors, suspicious attachments, strange domain names, use of the word “kindly”, etc.
- ACT IMMEDIATELY if you think you may have clicked on something suspicious

First American reports that 80% of listings for vacant/unencumbered property are fraudulent, so please be so careful with any of these deals that you get, not any for this specific property. That's a very scary percentage!

This excerpt is from their original Seller Impersonation Bulletin:

Advisory:

On all vacant, unencumbered land transactions, ASSUME IT IS FRAUD UNTIL YOU PROVE IT IS NOT. Additional due diligence is required to confirm that you are dealing with an authentic Seller. If you operate under split closings and have the Buyer's side of the transaction or are underwriting title only, it is still imperative you confirm the identity of the Seller has been verified. The following are some best practice techniques you can use to verify the validity of a Seller:

SELLER IMPERSONATION FRAUD
IN REAL ESTATE

FRAUDSTERS are impersonating property owners to illegally sell commercial or residential property. Sophisticated fraudsters are using the real property owner's Social Security and driver's license numbers in the transaction, as well as legitimate notary credentials, which may be applied without the notary's knowledge.

Fraudsters prefer to use email and text messages to communicate, allowing them to mask themselves and commit crime from anywhere.

Due to the types of property being targeted, it can take months or years for the actual property owner to discover the fraud. Property monitoring services offered by county recorder's offices are helpful, especially if the fraud is discovered prior to the transfer of money.

Where approved by state regulators, consumers can purchase the American Land Title Association (ALTA) Homeowner's Policy of Title Insurance for additional fraud protection.

WATCH FOR RED FLAGS

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A PROPERTY

- Is vacant or non-owner occupied, such as investment property, vacation property, or rental property
- Has a different address than the owner's address or tax mailing address
- Has no outstanding mortgage or liens
- Is for sale or sold below market value

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A SELLER

- Wants a quick sale, generally in less than three weeks, and may not negotiate fees
- Wants a cash buyer
- Is refusing to attend the signing and claims to be out of state or country
- Is difficult to reach via phone and only wants to communicate by text or email, or refuses to meet via video call
- Demands proceeds be wired
- Refuses or is unable to complete multifactor authentication or identity verification
- Wants to use their own notary

SHUTTERSTOCK / TANYA ANTUSENOK

alta.org

SELLER IMPERSONATION FRAUD
IN REAL ESTATE

TAKE PRECAUTIONS

CONTACT SELLER USING INDEPENDENT SOURCES

- Contact the seller directly at an independently discovered and validated phone number
- Mail the seller at the address on tax records, property address, and grantee address (if different)
- Ask the real estate agent if they have personal or verified knowledge of the seller's identity

MANAGE THE NOTARIZATION

- Require the notarization be performed by a vetted and approved remote online notary, if authorized in your state
- If remote online notarization is not available, the title company should select the notary. Examples include arranging for the seller to go to an attorney's office, title agency, or bank that utilizes a credential scanner or multifactor authentication to execute documents

VERIFY THE SELLER'S IDENTITY

- Send the seller a link to go through identity verification using a third-party service provider (credential analysis, KBA, etc.)
- Run the seller's email and phone number through a verification program
- Ask conversational questions to ascertain seller's knowledge of property information not readily available in public records
- Conduct additional due diligence as needed

USE THE PUBLIC RECORD

- Compare the seller's signature to previously recorded documents
- Compare the sales price to the appraisal, historical sales price, or tax appraisal value

CONTROL THE DISBURSEMENT

- Use a wire verification service or confirm wire instructions match account details on seller's disbursement authorization form
- Require a copy of a voided check with a disbursement authorization form
- Require that a check be sent for seller proceeds rather than a wire

FILE FRAUD REPORTS

- IC3.gov
- Local law enforcement
- State law enforcement, including the state bureau of investigation and state attorney general
- Secretary of state for notary violations

FIGHT FRAUD WITH INDUSTRY PARTNERS

- Educate real estate professionals in your community, such as country recorders, real estate agents, real estate listing platforms, banks, and lenders
- Host educational events at the local or state level
- Alert your title insurance underwriter of fraud attempts

SHUTTERSTOCK / TANYA ANTUSENOK

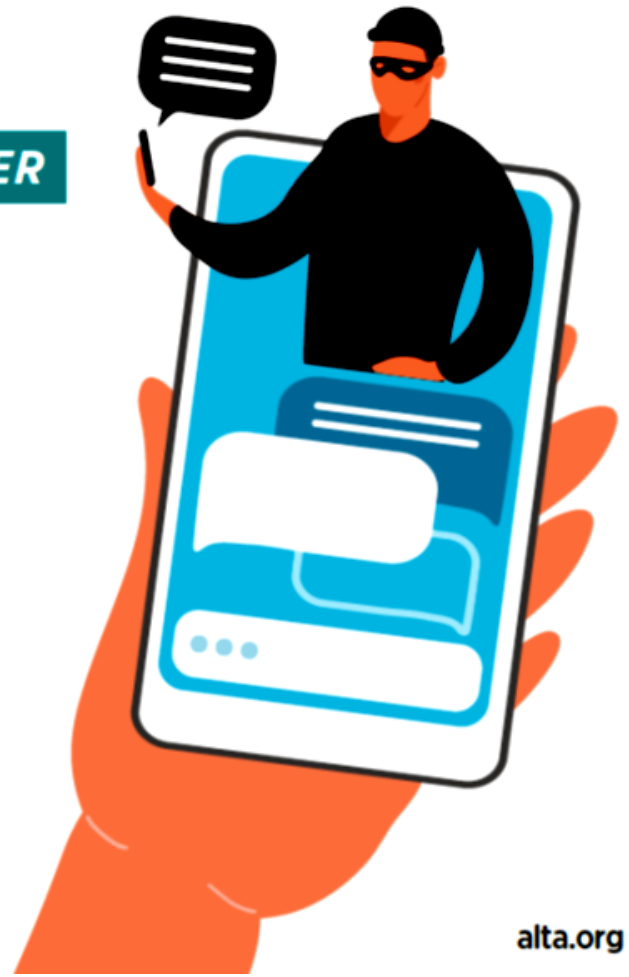
alta.org

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A PROPERTY

- Is vacant or non-owner occupied, such as investment property, vacation property, or rental property
- Has a different address than the owner's address or tax mailing address
- Has no outstanding mortgage or liens
- Is for sale or sold below market value

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A SELLER

- Wants a quick sale, generally in less than three weeks, and may not negotiate fees
- Wants a cash buyer
- Is refusing to attend the signing and claims to be out of state or country
- Is difficult to reach via phone and only wants to communicate by text or email, or refuses to meet via video call
- Demands proceeds be wired
- Refuses or is unable to complete multifactor authentication or identity verification
- Wants to use their own notary



SHUTTERSTOCK / TANYA ANTUSENOK

alta.org

SELLER IMPERSONATION FRAUD
IN REAL ESTATE

AMERICAN LAND TITLE ASSOCIATION

CONTACT THE SELLER USING INDEPENDENT SOURCES

- Contact the seller directly at an independently discovered and validated phone number
- Mail the seller at the address on tax records, property address, and grantee address (if different)
- Ask the real estate agent if they have personal or verified knowledge of the seller's identity

MANAGE THE NOTARIZATION

- Require the notarization be performed by a vetted and approved remote online notary, if authorized in your state
- If remote online notarization is not available, the title company should select the notary. Examples include arranging for the seller to go to an attorney's office, title agency, or bank that utilizes a credential scanner or multifactor authentication to execute documents

VERIFY THE SELLER'S IDENTITY

- Send the seller a link to go through identity verification using a third-party service provider (credential analysis, KBA, etc.)
- Run the seller's email and phone number through a verification program
- Ask conversational questions to ascertain seller's knowledge of property information not readily available in public records
- Conduct additional due diligence as needed

SELLER IMPERSONATION FRAUD IN REAL ESTATE

AMERICAN LAND TITLE ASSOCIATION

USE THE PUBLIC RECORD

- Compare the seller's signature to previously recorded documents
- Compare the sales price to the appraisal, historical sales price, or tax appraisal value

CONTROL THE DISBURSEMENT

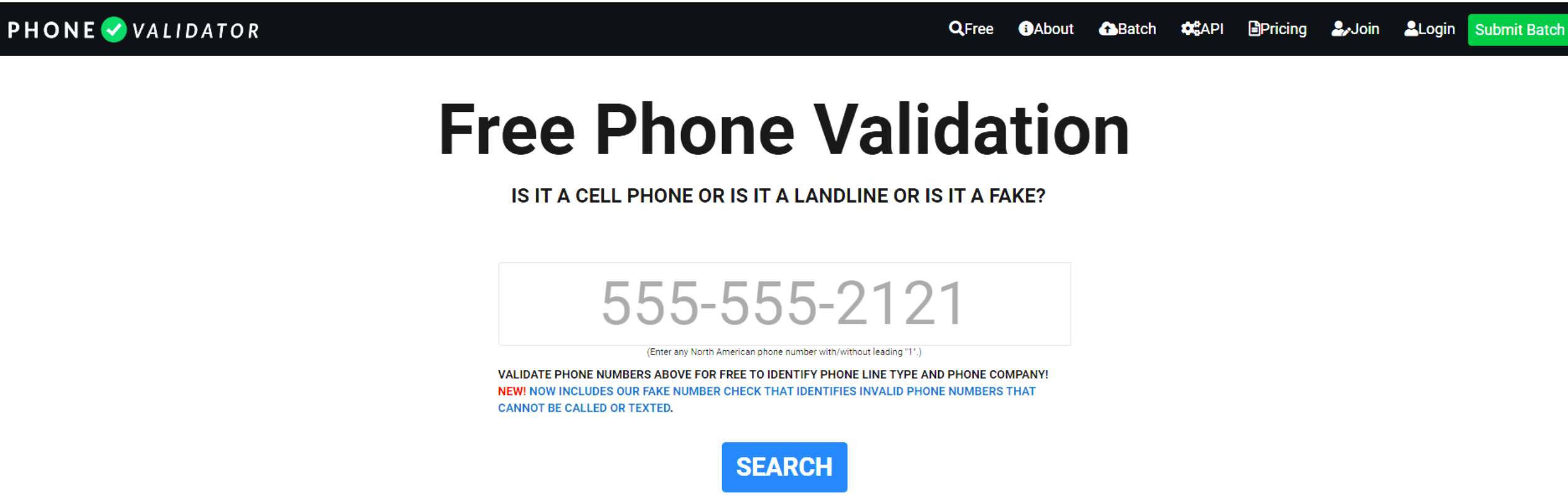
- Use a wire verification service or confirm wire instructions match account details on seller's disbursement authorization form
- Require a copy of a voided check with a disbursement authorization form
- Require that a check be sent for seller proceeds rather than a wire

FIGHT FRAUD WITH INDUSTRY PARTNERS

- Educate real estate professionals in your community, such as country recorders, real estate agents, real estate listing platforms, banks, and lenders
- Host educational events at the local or state level
- Alert your title insurance underwriter of fraud attempts

FILE FRAUD REPORTS

- IC3.gov
- Local law enforcement
- State law enforcement, including the state bureau of investigation and state attorney general
- Secretary of state for notary violations



https://phonevalidator.com/index.aspx

Cells

Landlines

VOIP

We are the experts for phone number lookups to determine phone line type. Do you need to know if phone numbers are mobile, landline, toll-free, VOIP, fake/invalid? Our phone number API covers all line types and all U.S phone companies! Run a phone number search above to see our uncanny accuracy. Sign up for a free trial today!

Works with Numbers from All U.S. Phone Companies*

at&t	COMCAST	Sprint	T-Mobile
TRACFONE wireless, inc.	verizon	metroPCS	Vonage

*All phone company logos are trademarks of their respective companies. No affiliation or endorsement of this website or service exists. Logos are for the purpose of describing the capabilities of this service only.

https://phonevalidator.com/index.aspx

UNDERWRITING CHALLENGE

LANGUAGE FINGERPRINTS

Did you know you can spot a fraudster just by the way they write? Fraudsters often leave traces of their crime behind in their language fingerprints. Language fingerprints can be found in emails, letters, transaction documents, wire instructions, and payoff statements. Knowing what words fraudsters use and how they use them can help you spot and stop a crime happening right before your eyes.

Fraudster Lexicon

There are certain words or types of words used frequently by fraudsters to manipulate you into doing what they want. If you spot the fraudster's lexicon, please STOP to review the transaction as a whole and consider you may be dealing with a fraudster.

"Kindly"

The #1 word used by fraudsters is "kindly." Most cybercrime is committed by overseas fraudsters where this word is part of their vernacular instead of the word "please." If someone uses the word "kindly" or uses it repeatedly in one communication, chances are you are communicating with a fraudster.

Words indicating friendship

Words of friendship convey familiarity, trust, and can include someone being overly complimentary about your role in the transaction. The fraudsters use this technique to lower your guard by playing on your ego's desire to be liked. You are more likely to go the extra mile for a "friend" or "pal" and overlook discrepancies and red flags for people you like and trust.

Risk Words

Risk words imply a possible negative action or outcome to you personally and at their core are a latent threat to your financial security invoking a fear response. Risk words including "concern," "prevent," "failure," and "avoid" all imply there are consequences to not following the request.

Negative words

Any instruction you receive that tells says you "must not," "shall not," "never," "do not do [something]" is a red flag. Consider what it is they are instructing you not to do and if it makes sense in the transaction. Do they not want you to verify something, call or email someone specific, or not use a telephone or email address you previously used throughout the transaction?

God or religion-type words

Culturally, words with religious overtones are not used in real estate transactions in the United States, but that isn't necessarily the case in foreign countries. If someone refers to God or uses other words with religious overtones in an email or any written communication, consider a fraudster from a country where that is acceptable or even expected in a business transaction may be impersonating a party.

Fraudster Grammar

Since most cybercrime originates from overseas, the fraudster may have a poor command of the English language and grammar. Communications or instructions that contain any of the following grammatical errors are a red flag for fraud:

- Missed punctuation
- Misuse of punctuation
- Misspelled words
- Incorrect spacing or formatting
- Capitalization errors
- Improper syntax
- Improper verb usage
- Improper verb tense usage

Wire Instructions

Wire instructions and payoff statements can contain language fingerprints too! Be on the lookout for:

- Different font or type size from the rest of the document
- Sender's location shown on a faxed document does not match party's purported location
- Payoff amount differs from a previously received payoff statement or calculation of payoff amount doesn't add up
- Receiving bank does not match payoff statement bank
- Beneficiary's name on the account differs from party or lender
- Address or phone number listed in the statement is different than contact information that is independently verified
- Email address is different or contains variations
- Rush requests or sense of urgency
- Wire is going to a bank in a country outside of US or different from where the party is located

ALWAYS carefully compare updated payoff statements with the original one and be suspect of last minute changes in wire instructions.

If you suspect fraud, escalate to your management or contact your state underwriter for additional review.

First American Title™

800.854.3643 ▾ www.firstam.com

FAT-05/2022

Fraudster Grammar

Since most cybercrime originates from overseas, the fraudster may have a poor command of the English language and grammar. Communications or instructions that contain any of the following grammatical errors are a red flag for fraud:

- Missed punctuation
- Misuse of punctuation
- Misspelled words
- Incorrect spacing or formatting
- Capitalization errors
- Improper syntax
- Improper verb usage
- Improper verb tense usage

UNDERWRITING CHALLENGE

LANGUAGE FINGERPRINTS

Did you know you can spot a fraudster just by the way they write? Fraudsters often leave traces of their crime behind in their language fingerprints. Language fingerprints can be found in emails, letters, transaction documents, wire instructions, and payoff statements. Knowing what words fraudsters use and how they use them can help you spot and stop a crime happening right before your eyes.

Fraudster Lexicon

There are certain words or types of words used frequently by fraudsters to manipulate you into doing what they want. If you spot the fraudster's lexicon, please STOP to review the transaction as a whole and consider you may be dealing with a fraudster.

"Kindly"

The #1 word used by fraudsters is "kindly." Most cybercrime is committed by overseas fraudsters where this word is part of their vernacular instead of the word "please." If someone uses the word "kindly" or uses it repeatedly in one communication, chances are you are communicating with a fraudster.

Words indicating friendship

Words of friendship convey familiarity, trust, and can include someone being overly complimentary about your role in the transaction. The fraudsters use this technique to lower your guard by playing on your ego's desire to be liked. You are more likely to go the extra mile for a "friend" or "pal" and overlook discrepancies and red flags for people you like and trust.

Risk Words

Risk words imply a possible negative action or outcome to you personally and at their core are a latent threat to your financial security invoking a fear response. Risk words including "concern," "prevent," "failure," and "avoid" all imply there are consequences to not following the request.

Negative words

Any instruction you receive that tells says you "must not," "shall not," "never," "do not do [something]" is a red flag. Consider what it is they are instructing you not to do and if it makes sense in the transaction. Do they not want you to verify something, call or email someone specific, or not use a telephone or email address you previously used throughout the transaction?

God or religion-type words

Culturally, words with religious overtones are not used in real estate transactions in the United States, but that isn't necessarily the case in foreign countries. If someone refers to God or uses other words with religious overtones in an email or any written communication, consider a fraudster from a country where that is acceptable or even expected in a business transaction may be impersonating a party.

Fraudster Grammar

Since most cybercrime originates from overseas, the fraudster may have a poor command of the English language and grammar. Communications or instructions that contain any of the following grammatical errors are a red flag for fraud:

- Missed punctuation
- Misuse of punctuation
- Misspelled words
- Incorrect spacing or formatting
- Capitalization errors
- Improper syntax
- Improper verb usage
- Improper verb tense usage

Wire Instructions

Wire instructions and payoff statements can contain language fingerprints too! Be on the lookout for:

- Different font or type size from the rest of the document
- Sender's location shown on a faxed document does not match party's purported location
- Payoff amount differs from a previously received payoff statement or calculation of payoff amount doesn't add up
- Receiving bank does not match payoff statement bank
- Beneficiary's name on the account differs from party or lender
- Address or phone number listed in the statement is different than contact information that is independently verified
- Email address is different or contains variations
- Rush requests or sense of urgency
- Wire is going to a bank in a country outside of US or different from where the party is located

ALWAYS carefully compare updated payoff statements with the original one and be suspect of last minute changes in wire instructions.

If you suspect fraud, escalate to your management or contact your state underwriter for additional review.

First American Title™

800.854.3643 ▾ www.firstam.com

FAT-05/2022

Wire Instructions - Wire instructions and payoff statements can contain language fingerprints too! Be on the lookout for:

- Different font or type size from the rest of the document
- Sender's location shown on a faxed document does not match party's purported location
- Payoff amount differs from a previously received payoff statement or calculation of payoff amount doesn't add up
- Receiving bank does not match payoff statement bank
- Beneficiary's name on the account differs from party or lender
- Address or phone number listed in the statement is different than contact information that is independently verified
- Email address is different or contains variations
- Rush requests or sense of urgency
- Wire is going to a bank in a country outside of US or different from where the party is located

ALWAYS carefully compare updated payoff statements with the original one and be suspect of last-minute changes in wire instructions.

If you suspect fraud, escalate to your management or contact your state underwriter for additional review.

Backman Title Services
www.backmantitle.com

Title Insurance & Property Watch

Are Title Thieves Really Stealing Utah Homes?

QR for KSL-TV Story

If you've come across those infomercials touting services that promise to protect homeowners from fraudulent title theft, you might be wondering about the actual likelihood of such an event occurring. Rest assured, while title fraud is indeed a possibility, it's an exceptionally rare and unlikely occurrence.

In fact, earlier this year, several reputable local media outlets delved into the subject, seeking insights from experts. A notable example is KSL-TV's Matt Gephardt and Sloan Schrage, who explored the truth behind claims of title thieves in this eye-opening piece:

www.ksl.com/article/50334898/ads-claim-title-thieves-can-steal-your-home-but-can-you-really-lose-your-house

Benefits of Title Insurance – Built in coverage for marketable title, fraud & forgery

While the news coverage shed light on this issue, it's worth noting that numerous homeowners are already safeguarded by their title insurance policies, often acquired at the time of property purchase. An Owner's policy encompasses protection against unmarketable titles, and many policies obtained since 2008 have extended coverage that includes safeguarding against post-policy forgery, fraud, and title-related complications. The specifics of coverage can vary, and deductibles might apply depending on the policy type. Remarkably, many policyholders could potentially have coverage that reaches up to 150% of their property's original purchase price.

Property Watch - Free service in some counties

For homeowners seeking a proactive approach to staying informed about their property's status, the Property Watch service is a remarkable resource available in select Utah counties. This service allows residents to stay in the loop about any recorded changes affecting their property. Once you enroll, you'll receive email notifications whenever a document is recorded that impacts your property's status.

Currently, this service is available in the following Utah counties:

Washington: https://www.washco.utah.gov/2021/11/04/sign-up-for-property-watch/
Salt Lake: https://slco.org/data-services/PropertyWatch/PropertyWatch.aspx
Uintah: https://co.uintah.ut.us:8443/ords/ucdev/r/property-watch-signup/home
Weber: https://www.webercountyutah.gov/forms/property_watch/
Cache: https://www.cachecounty.org/recorder/propertywatch/faq.html
Utah: https://property-watch.utahcounty.gov/
Daggett: https://www.daggettcounty.org/CivicAlerts.aspx?AID=1324
Uintah: https://apps.uintah.utah.gov/ords/ucdev/r/property-watch-signup/home

While the fear of title theft might be a headline-grabbing concern, the reality is that this type of fraud is an anomaly rather than the norm. Existing title insurance policies offer significant protection for homeowners, and the Property Watch service provides a valuable tool for staying informed about changes to your property.

Corporate Fraud Watch

The Utah Division of Corporations and Commercial Code provides a service to assist businesses in monitoring and receiving notifications regarding changes to their corporate information. These changes may be indicative of identity theft or fraudulent activities. The State promptly sends an email within 24 hours of any modification to a Business Address, Registered Agent, or Registered Principal. The cost for this service is $3.00 per year.
https://secure.utah.gov/fraudalert/

The Property Watch service is a remarkable resource available in select Utah counties. This service allows residents to stay in the loop about any recorded changes affecting their property. Once you enroll, you'll receive email notifications whenever a document is recorded that impacts your property's status.

Currently, this service is available in the following Utah counties:

Washington: https://www.washco.utah.gov/2021/11/04/sign-up-for-property-watch/
Salt Lake: https://slco.org/data-services/PropertyWatch/PropertyWatch.aspx
Weber: https://www.webercountyutah.gov/forms/property_watch/
Cache: https://www.cachecounty.org/recorder/propertywatch/faq.html
Utah: https://property-watch.utahcounty.gov/
Daggett: https://www.daggettcounty.org/CivicAlerts.aspx?AID=1324
Uintah: https://apps.uintah.utah.gov/ords/ucdev/r/property-watch-signup/home

While the fear of title theft might be a headline-grabbing concern, the reality is that this type of fraud is an anomaly rather than the norm. Existing title insurance policies offer significant protection for homeowners, and the Property Watch service provides a valuable tool for staying informed about changes to your property.