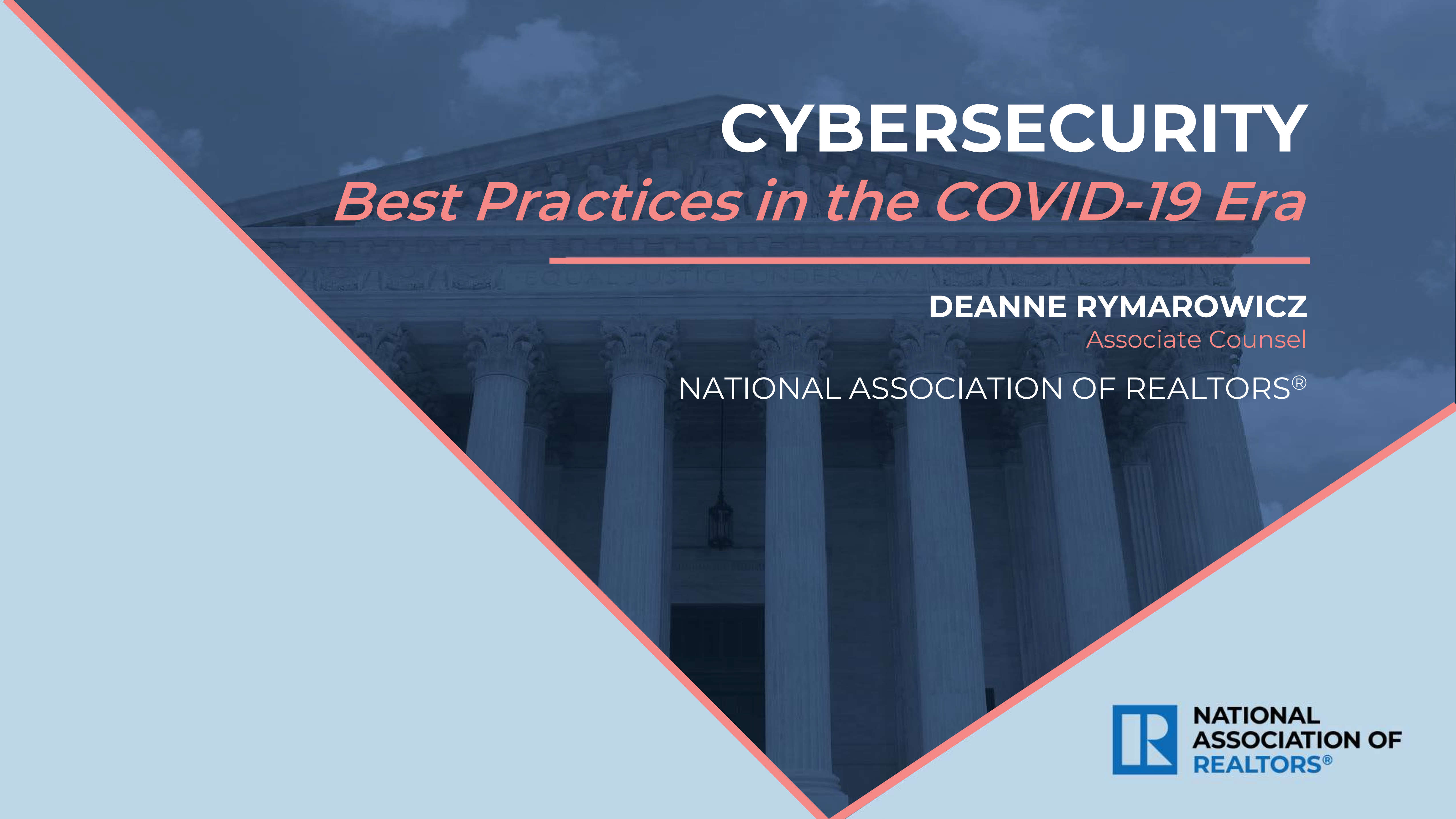


CYBERSECURITY

Best Practices in the COVID-19 Era

DEANNE RYMAROWICZ
Associate Counsel

NATIONAL ASSOCIATION OF REALTORS®

NATIONAL ASSOCIATION OF REALTORS®

OVERVIEW

- **Cybercrime in 2020**
  - Liability
  - What you need to know
- **Real Estate Wire Fraud**
  - Best practices
- **Ransomware**
- **Resources**

top:1%;position:abso
(o.createElement("div")),
display:inline;zoom:1",
null,t}();var O=
(p[f]={},l||(p[f].toJSON
acceptData(e)){var r,i,o,
}(n||(delete s[u].data,
(e){return e=e.nodeType
!==e.nodeType)
))){for(r=o.attr
(){b.data(this,e,n)}),
===r?!0:"false"===r?!
e?(n=(n||"fx")+"queue
===i&&(i=n.shift(),
(e,n)})})}}),b.fn.
unction(e){
,o=b.Deferred(),
on|object)
t,argume
(){

CYBERCRIME

CYBERSECURITY

is ________________.

NATIONAL
ASSOCIATION OF
REALTORS®

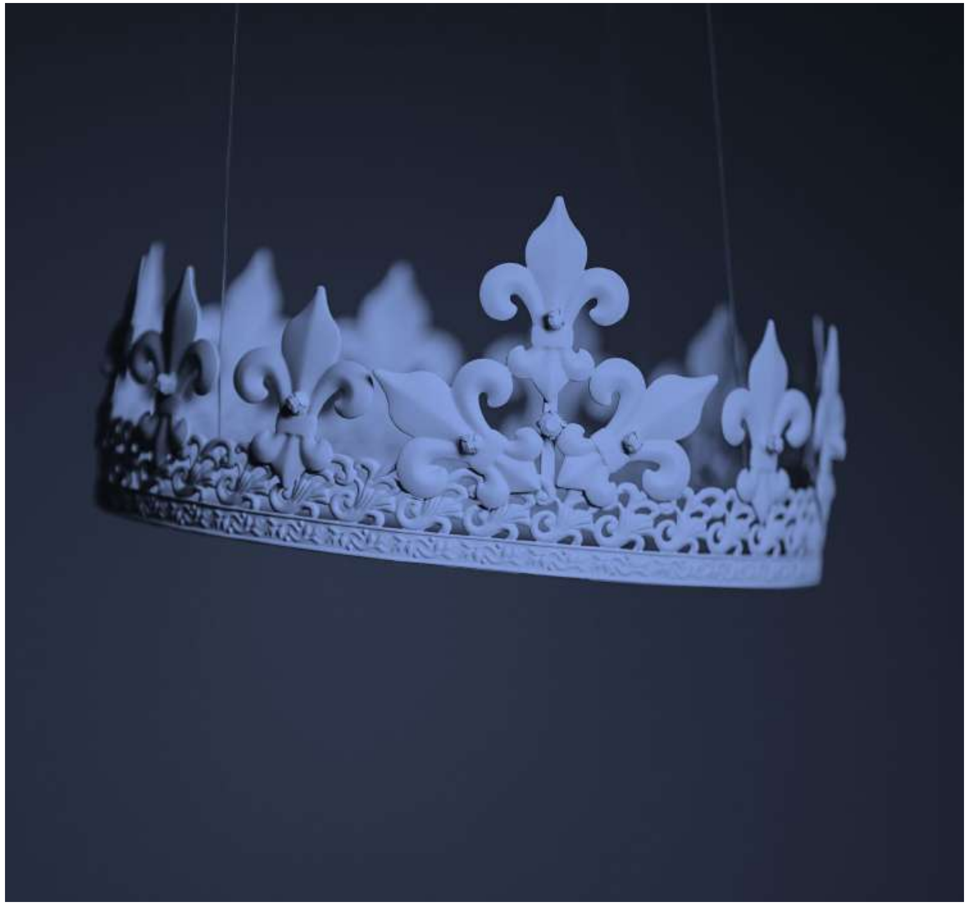
CYBERSECURITY

is an ***opportunity.***

NATIONAL
ASSOCIATION OF
REALTORS®

an **OPPORTUNITY** *to educate*

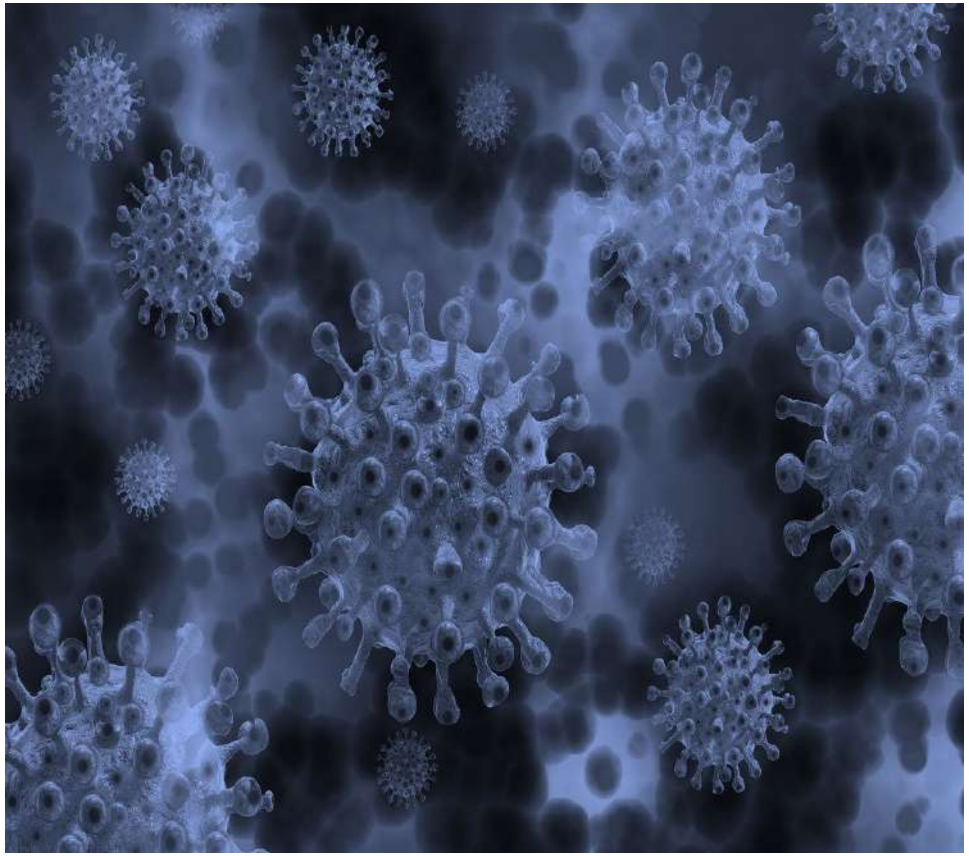
- YOURSELF
- STAFF
- AGENTS/TEAM
- CLIENTS



Once upon a time, there was a long lost African prince ….

NATIONAL ASSOCIATION OF REALTORS®

… and then one day, along came COVID.



NATIONAL ASSOCIATION OF REALTORS®

CYBERCRIME BY THE NUMBERS

2,211,396

scam complaints 2016-2020

Source: 2020 IC3 Internet Crime Report

NATIONAL ASSOCIATION OF REALTORS®

CYBERCRIME BY THE NUMBERS

$ **13.3 billion**

total reported
losses 2016-2020

Source: 2020 IC3 Internet Crime Report

CYBERCRIME BY THE NUMBERS

COMPLAINTS FILED IN 2020

2,169 A DAY

A TOTAL OF

791,790

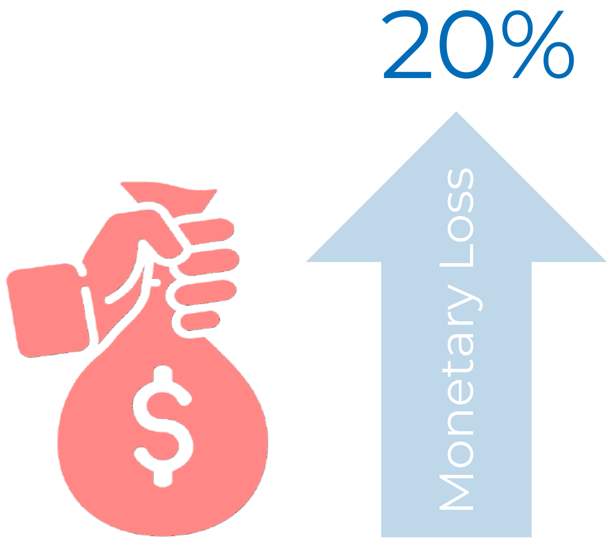
FOR THE YEAR

$4.2 BILLION

Source: *2020 IC3 Internet Crime Report*

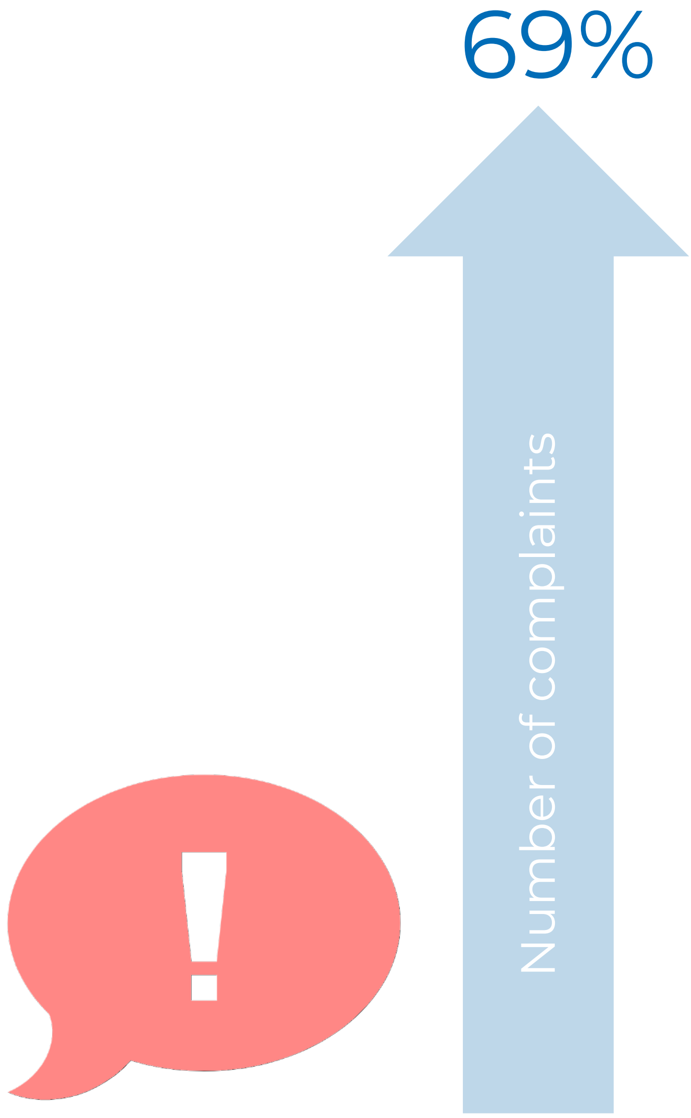
CYBERCRIME BY THE NUMBERS

YEAR OVER YEAR, 2019-2020



20%

Monetary Loss



69%

Number of complaints

Source: 2020 IC3 Internet Crime Report

CYBERCRIME BY THE NUMBERS

COVID-SPECIFIC CYBERCRIMES

- **Increased reliance on technology**
  - Telecommuting
  - More digital communications and transactions

- **Specific COVID-related fraud**
  - More than 28,500 complaints
  - Typically impersonating a government rep
  - Now turning to vaccine fraud

CYBERCRIME BY THE NUMBERS

COVID-SPECIFIC CYBERCRIMES

- **Frauds based on government relief**
  - PPP loans
  - Unemployment benefits
  - Information about stimulus checks
- **Medical workers searching for PPE**

Source: 2020 IC3 Internet Crime Report

CYBERCRIME BY THE NUMBERS

TOP CYBERCRIME CATEGORIES BY LOSS - 2020

1. Email compromise
2. Confidence/ Romance
3. Investment
4. Non-payment/ non-delivery
5. Identity theft
6. Spoofing
7. Real estate/rental fraud → #7 OUT OF 33 CATEGORIES!

Source: 2020 IC3 Internet Crime Report

CYBERCRIME BY THE NUMBERS

GUAM

112

victims

Source: 2020 IC3 Internet Crime Report

NATIONAL ASSOCIATION OF REALTORS®

CYBERCRIME BY THE NUMBERS

GUAM

$259,339

total loss

Source: 2020 IC3 Internet Crime Report

NOTABLE CASES

O'Neill, Bragg & Staff, PC v. Bank of America

The bank is not an agent of the law firm and did not owe any fiduciary or special duty to the law firm to stop a fraudulent wire transfer.

97 UCC Rep.Serv.2d 212 (2018)

NATIONAL ASSOCIATION OF REALTORS®

NOTABLE CASES

Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.

In determining which party bears the risk of loss resulting from wire fraud, courts should consider which party was in the best position to prevent the fraud.

759 Fed.Appx. 348 (2018)

NOTABLE CASES

Jetcrete North America v. Austin Truck & Equipment

A rigid standard of strict liability for damages arising from a hacked email account is not practical; no email platform is impervious to hacking. Both sides must use reasonable care to avoid losses.

484 F.Supp.3d 915 (2020)

CYBERCRIME – WHAT TO KNOW

Hover your mouse over the sender's address and the link address to discover the true sender/destination.

COPY (do not click!) the link and run it through a detection site like:

- Urlscan.io
- Virustotal.com
- Urlvoid.com
- Isitphishing.org

Call the sender to verify the email and the link is from them. Do not reply to an email … you could be emailing the hacker!

NATIONAL ASSOCIATION OF REALTORS®

CYBERCRIME – WHAT TO KNOW

Awareness is the key.

- The more you know about current cyber threats and their implications the more you can protect you and your clients.
- Visit IC3.gov for the latest info on scams.
- Stay vigilant with emails and online transactions.
- Do not give out personal information!

Prevention needs to become a routine activity.

- Remember the basics like ensuring OS and firewall are up to date.

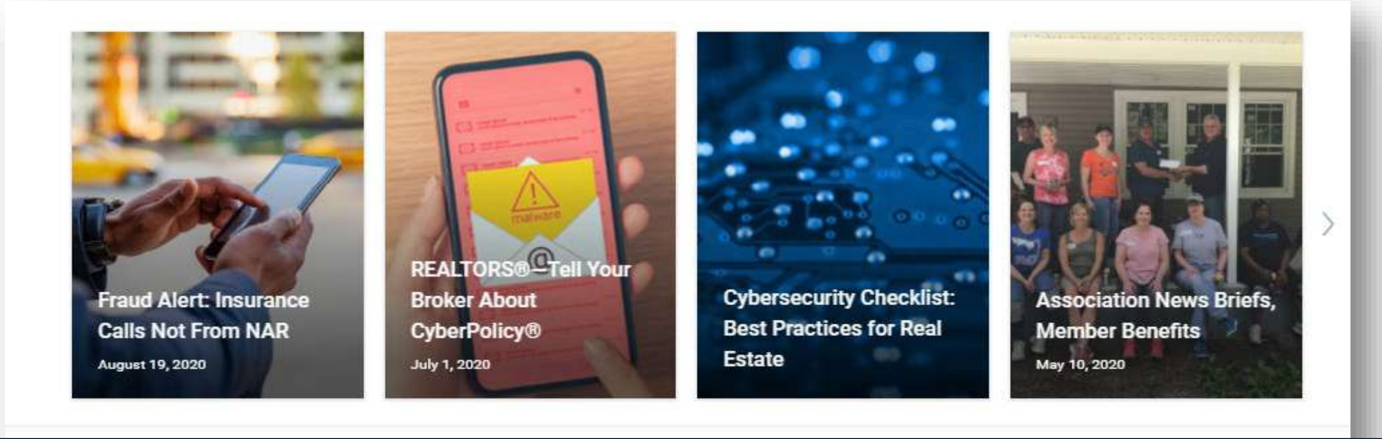
CYBERCRIME – WHAT TO KNOW

Common sense is your friend!

Always use: Stop, Wait, Does this make sense?

- Would this person normally email you with that request?
- Does your bank ask you to send them your password?
- Does this sound like a client you have been working with?
- Were you expecting this attachment from your colleague?

NAR RESOURCES



Fraud Alert: Insurance Calls Not From NAR

August 19, 2020

REALTORS®—Tell Your Broker About CyberPolicy®

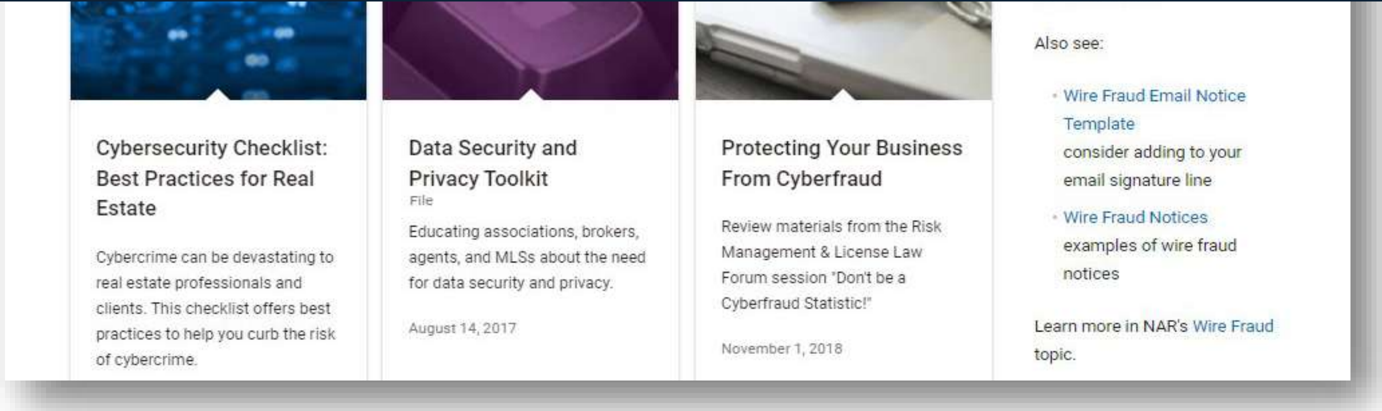
July 1, 2020

Cybersecurity Checklist: Best Practices for Real Estate

Association News Briefs, Member Benefits

May 10, 2020

nar.realtor/data-privacy-security



Cybersecurity Checklist: Best Practices for Real Estate

Cybercrime can be devastating to real estate professionals and clients. This checklist offers best practices to help you curb the risk of cybercrime.

Data Security and Privacy Toolkit

File

Educating associations, brokers, agents, and MLSs about the need for data security and privacy.

August 14, 2017

Protecting Your Business From Cyberfraud

Review materials from the Risk Management & License Law Forum session "Don't be a Cyberfraud Statistic!"

November 1, 2018

Also see:

- Wire Fraud Email Notice Template
  consider adding to your email signature line
- Wire Fraud Notices
  examples of wire fraud notices

Learn more in NAR's Wire Fraud topic.

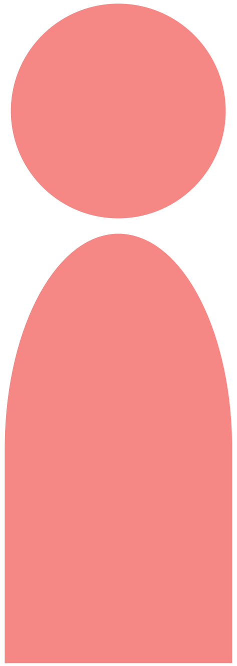
REAL ESTATE WIRE FRAUD

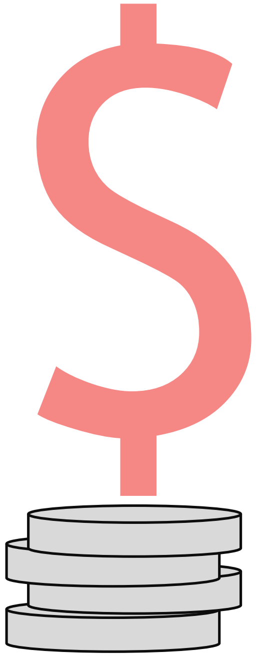
NATIONAL
ASSOCIATION OF
REALTORS®

REAL ESTATE WIRE FRAUD

13,638
VICTIMS

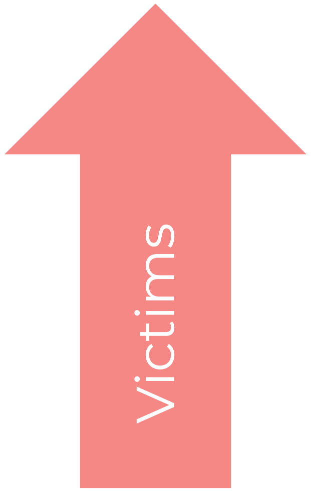
$213.2 M
TOTAL LOSSES

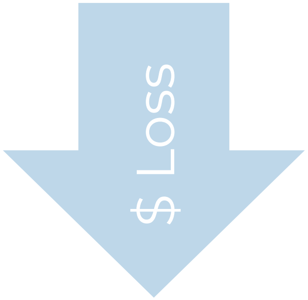




IN 2020

16.8%





3.7%

YEAR OVER YEAR

Source: 2020 IC3 Internet Crime Report

NATIONAL
ASSOCIATION OF
REALTORS®

REAL ESTATE WIRE FRAUD

WATCH

PROFILE

HACK

STEAL

NOTABLE CASES

Bain v. Platinum Realty, LLC

Agent claimed she never sent the fraudulent wire instructions but confirmed to buyer to wire money before closing. Jury found real estate agent 85% liable. Judgment of $167,129 entered against brokerage.

2018 WL 3105376 (2018)

RECOMMENDED PRACTICES

Educate buyers about possible scams.

NATIONAL ASSOCIATION OF REALTORS®

PROTECT YOUR MONEY FROM MORTGAGE CLOSING SCAMS WHEN BUYING A HOME

Every day, hackers try to steal your money by emailing fake wire instructions. Criminals will use a similar-looking (*but fake*) email address and steal a logo and other info to make it look like the email came from your real estate agent or title company. **You can protect yourself & your money by following these steps:**

BE VIGILANT

Call, don't click: Verify all wiring instructions before transferring your funds. Call the title company using an independently obtained and known phone number. Don't use phone numbers or links from an email.

Be aware: It's extremely rare that wiring instructions will change at the last minute, or that this information will be provided by email.

PROTECT YOUR MONEY

Confirm everything: Ask your bank to confirm the name on the receiving account before sending a wire.

Verify Immediately: Within four to eight hours, call the title company or real estate agent to confirm they received your money.

WHAT TO DO IF YOU'VE BEEN TARGETED

IMMEDIATELY:

- ✓ **Call** your bank and ask them to issue a recall notice for your wire.
- ✓ **File** a complaint with the FBI at www.IC3.gov.
- ✓ **Report** the crime to your local FBI office.

Making a report within the first 24 hours provides the best chance of recovering your money.

For more information about mortgage closing scams, please visit: **NAR.REALTOR/WIRE-FRAUD**

This is for informational purposes only and should not be considered legal advice.

American Land Title Association
Protect your property rights

NATIONAL ASSOCIATION of REALTORS®

- Free in the REALTOR® Store.
- Printable!

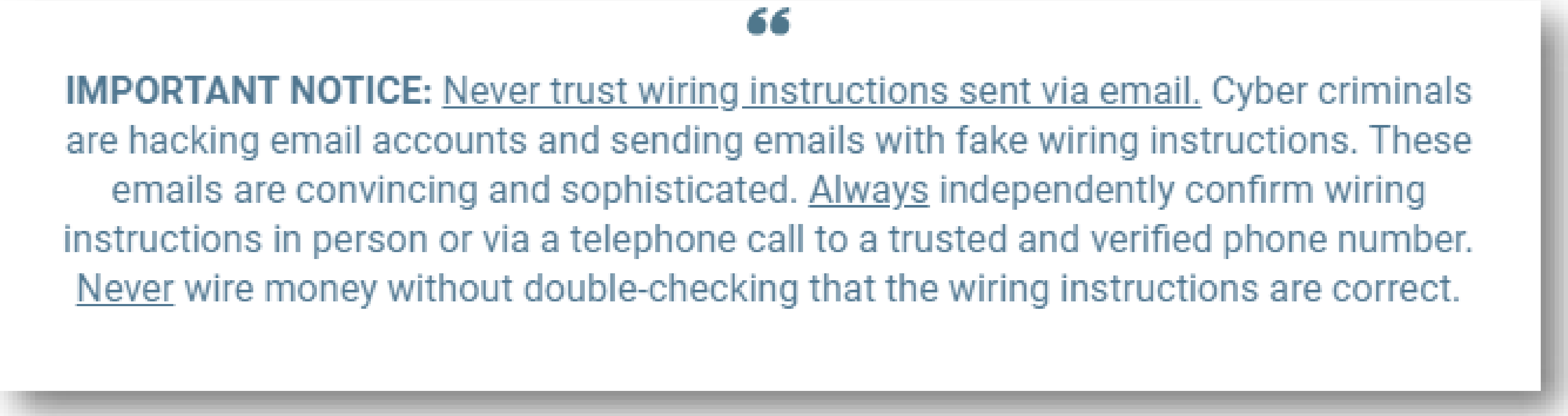
RECOMMENDED PRACTICES

- ✓ Use a transaction management platform or secure email to communicate with clients.
- ✓ Never send wire instructions via e-mail.
- ✓ Verify instructions with a phone number independent ly obtained.
- ✓ Use smart email practices.

NATIONAL ASSOCIATION OF REALTORS®

RECOMMENDED PRACTICES

Include a wire fraud notice in your email signature.



❝

IMPORTANT NOTICE: Never trust wiring instructions sent via email. Cyber criminals are hacking email accounts and sending emails with fake wiring instructions. These emails are convincing and sophisticated. Always independently confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. Never wire money without double-checking that the wiring instructions are correct.

Email Notice Template available on nar.realtor: https://www.nar.realtor/law-and-ethics/wire-fraud-email-notice-template

RECOMMENDED PRACTICES

✓

Use strong passwords for your email and all online accounts.

RECOMMENDED PRACTICES

Consider an insurance policy that covers client (third party) losses.

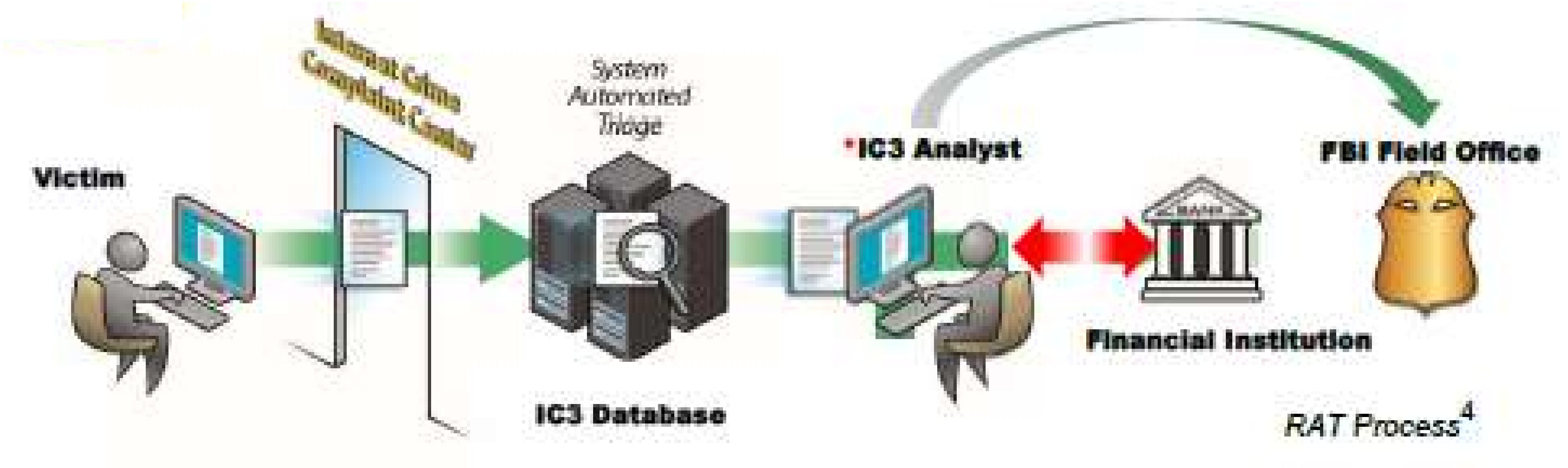
Cyber Insurance
Designed specifically for the real estate industry.
LEARN MORE
CyberPolicy
NATIONAL ASSOCIATION OF REALTORS®
REALTOR BENEFITS® PROGRAM

Learn more: nar.realtor/cyberpolicy

IF FRAUD OCCURS

- ✓ Notify the other parties.
- ✓ Contact the bank immediately.
- ✓ File a complaint with the FBI at IC3.gov.
- ✓ Report to the local FBI office.

IF FRAUD OCCURS



Of 1,303 incidents forwarded to RAT in 2020, **82%** of funds were recovered.

Source: 2020 IC3 Internet Crime Report

NATIONAL ASSOCIATION OF REALTORS®

RESOURCES

Wire Fraud

Emilija Manevska / Moment / Getty Images

One of the fastest growing cybercrimes in the U.S. is wire fraud in real estate. About 11,677 people were victims of wire fraud in the real estate and rental sector in 2019 with losses of more than $221 million (a 48% increase over 2018), according to FBI data. That ranks real estate and rental wire fraud #5 out of more than 30 types of fraud tracked by the FBI's Internet Crime Complaint Center.

The highest reported fraud in real estate in 2019 was Business Email Compromise/Email Account Compromise (BEC/EAC.) Fraudsters will assume the identity of the title, real estate agent or closing attorney and forge the person's email and other details about the transaction. The scammers will then send an email to the unknowing buyer and provide new wire instructions to the criminal's bank account.

Based on victim complaint data, BEC/EAC scams targeting the real estate sector continue to rise. From calendar year 2015 to calendar year 2017, there was over an 1100% rise in the number of BEC/EAC victims reporting the real estate transaction angle and an almost 2200% rise in the reported monetary loss Victims participating at all levels of a real estate transaction have reported such activity to the Internet Crime Complaint Center.[1]

nar.realtor/wire-fraud

NAR RESOURCES

Window to the Law: https://www.nar.realtor/videos/window-to-the-law/window-to-the-law-creating-a-cybersecurity-program

Cybersecurity Checklist: https://www.nar.realtor/law-and-ethics/cybersecurity-checklist-best-practices-for-real-estate-professionals

Mortgage Closing Scam Client Brochure: https://store.realtor/mortgage-closing-scam-client-advisory-brochure-download/

Data Security and Privacy Toolkit: https://www.nar.realtor/data-privacy-security/nars-data-security-and-privacy-toolkit

Wire Fraud Notice Template: https://www.nar.realtor/law-and-ethics/wire-fraud-email-notice-template

IC3 2020 Internet Crime Report:
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

NATIONAL ASSOCIATION OF REALTORS®

RANSOMWARE

NATIONAL
ASSOCIATION OF
REALTORS®

RANSOMWARE BY THE NUMBERS

2,474 COMPLAINTS

$29.1+ million
(likely a low number)

486% increase
2018-2022

WHAT IS RANSOMWARE?

- Malicious software (Malware)
- Denies access to a system or data until a ransom is paid
- Locker Ransomware
    - Blocks access to a system or device
- Crypto Ransomware
    - Prevents access to files and data through encryption
- In addition to holding a decryption key, will threaten to sell or leak exfiltrated data or sensitive information if ransom isn’t paid

NATIONAL ASSOCIATION OF REALTORS®

RANSOMWARE IN THE NEWS

CNA Financial

- Attacked on March 21 by Phoenix CryptoLocker
- Over 15,000 devices were encrypted, and systems were down until May 12
- Paid a reported $40M ransom

Colonial Pipeline

- Attacked on May 7 by Darkside ransomware gang
- Forced to shut down operations, disrupting fuel supply to east coast states until May 12
- Paid $4.4M ransom

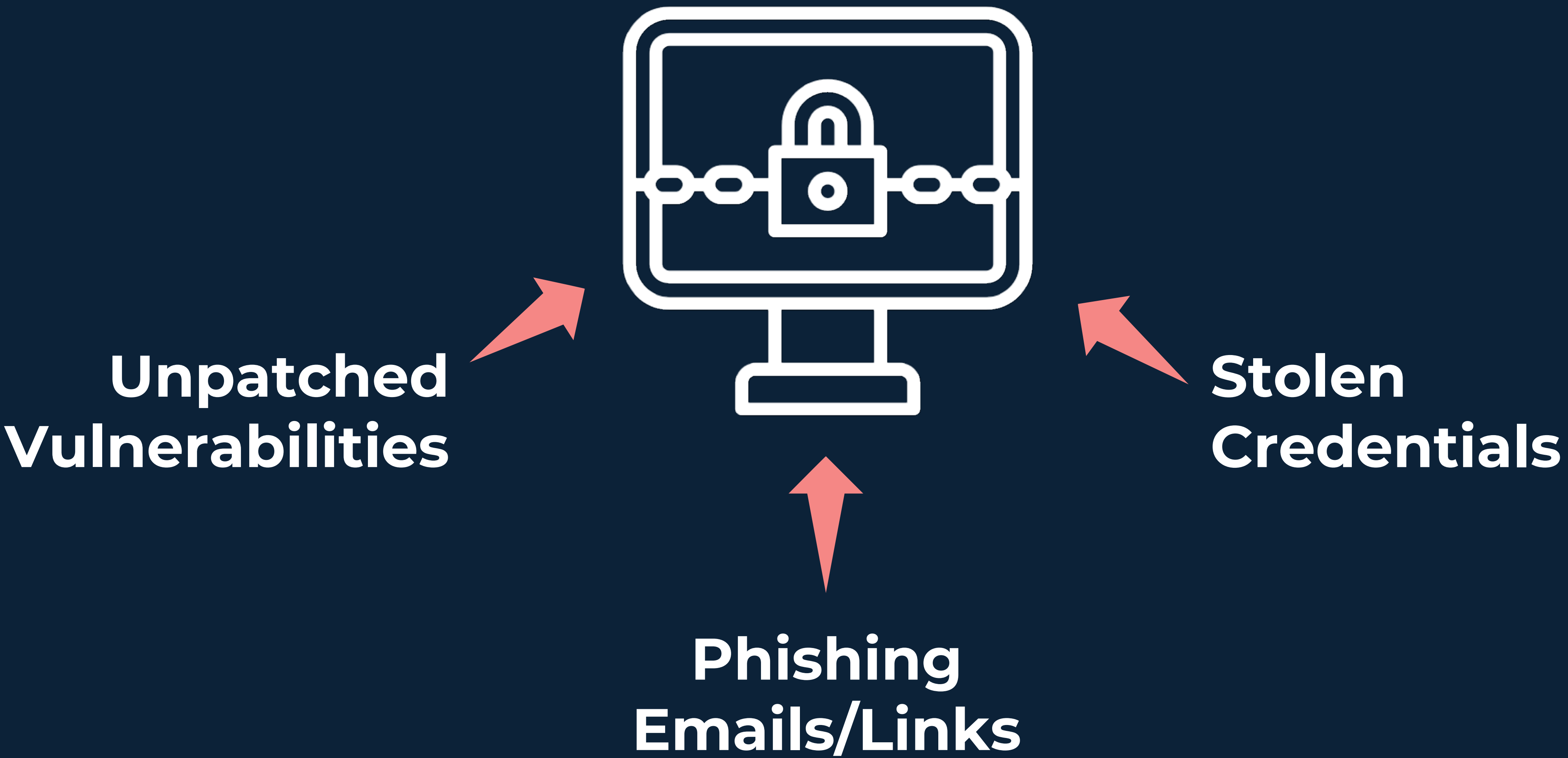
JBS USA

- Attacked on May 30 by REvil ransomware
- Forced to shut down operations 13 days
- Paid $11M ransom

IMPACT OF RANSOMWARE

- Disruption to production, delivery, or customer services
- Loss of sensitive commercial data, or protected information
- Direct costs of remediation, recovery, or potential ransom payment
- Costs associated with litigation, often class-action lawsuits
- Legal and regulatory sanctions
- Reputational damage

HOW DO YOU GET RANSOMWARE?



Unpatched Vulnerabilities

Stolen Credentials

Phishing Emails/Links

BEST PRACTICES

- Know what your most critical systems and data are.

- Review (or create) a systems recovery/disaster preparedness plan. Work with an IT professional as needed.

- Ensure your firewall is secure, and anti-virus software is updated. (Remember those security patches!)

BEST PRACTICES

- Implement the 3-2-1 backup plan: have at least 3 copies of your data – 2 stored locally on different devices and 1 stored offsite.
- Train staff to recognize phishing emails. **DON'T CLICK LINKS!**
- Review insurance coverage and understand the limits and coverages for ransomware.

HOW TO HANDLE AN ATTACK

- ✓ Engage the response team
- ✓ Contain and isolate the affected systems or files
- ✓ Contact insurance and the authorities
- ✓ Preserve and analyze
- ✓ Restore access to systems
- ✓ Post incident assessment

NATIONAL ASSOCIATION OF REALTORS®

RESOURCES

White House Executive Order: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

US Government Stop Ransomware Website: https://www.cisa.gov/stopransomware

Secret Service Ransomware Guide:
https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident

IC3 Ransomware Fact Sheet:
https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf

Window to the Law: Create a Disaster Preparedness Plan:
https://www.nar.realtor/videos/window-to-the-law/create-a-disaster-preparedness-plan

THANK YOU.

DEANNE RYMAROWICZ
Associate Counsel

EMAIL ME
drymarowicz@nar.realtor

CALL ME
312-329-8386

NATIONAL
ASSOCIATION OF
REALTORS®