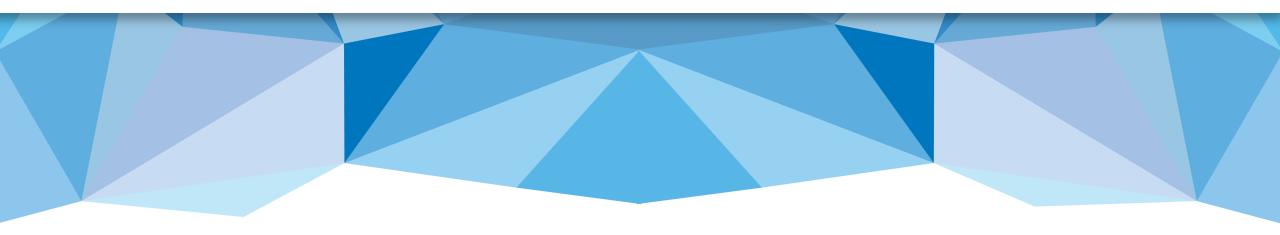


## Cybersecurity: What Brokers Need to Know

#### Melanie Wyne, Director, Federal Technology Policy, NAR





## Eat Your Vegetables

#### Security as a Business Differentiator

- Use Cybersecurity knowledge as another way to build trust with clients
- Have security discussions early and often (throughout the transaction)



## Cybersecurity in Context

- 53,000 incidents with 2, 216 confirmed breaches
- 73% by outsiders and 28% internal
  - 48% by hacking
  - 30% by malware
  - 17% via social attack
- 58% of attacks targeted small business
- Average cost of a breach to businesses was \$3.86 million



#### **Always New Incidents**

- June 2019: First American Title—885 Million records including mortgage docs found on open internet site
- June 2019: Metrolist MLS—Sacramento CA –MLS system taken down by ransomeware attack
- May 2019: City of Baltimore suffers ransomeware attack, RE closings halted for several days.

#### Know the Risks

- Wire Fraud/Phishing
- Ransomware
- Connected Homes
- Data Security Best Practices



### Real Estate Wire Fraud

- Based on FBI data in FY 2017 \$969 million was "diverted or attempted to be diverted" from a real estate transaction to criminally controlled accounts
- In 2016 the number of fraud cases jumped 480 percent
- Brokers may have legal liability if they fail to adequately warn consumers of wire fraud risk.



#### Wire Fraud Starts with Phishing

- Phishing relies on human engineering
- Slow down, trust your gut
- Verify urls/email addresses
- Beware free wi-fi
- Use encrypted email, transaction platforms





#### What to do if it Happens to You

- Call the bank—if caught w/in 24-48 hours funds may be recoverable
- Report to FBI www.ic3.gov
- Consider cyber insurance





#### Ransomware

- Keep a regular backup of your files
- Always keep your software updated
- Consider a Cyber Rider to your E&O policy



#### **Connected Home Security**

- Reset smart thermostats, locks, doorbells
- Replace devices that the manufacturer no longer supports







#### Data Security Best Practices

- Take Stock
- Know the Law
- Pitch It
- Lock it Down
- Have a Plan
- Train
- Password Hygiene
- Be a smart surfer



#### Know the Law

- No federal data security law—state regime
- Jurisdiction based on location of consumer not business
- WA has a data breach notification law
- 2019 expanded definition of personally identifiable information (HB 1071)—effective March 2020



## CA is Changing the Game

- CCPA Takes Effect Jan. 1 2020
- Consumers will have the right to:
  - Access and delete their personal information
  - Know what information has been collected, how it is used, to whom it is disclosed
  - Opt out of sale of personal information
- Private Right of Action for breach



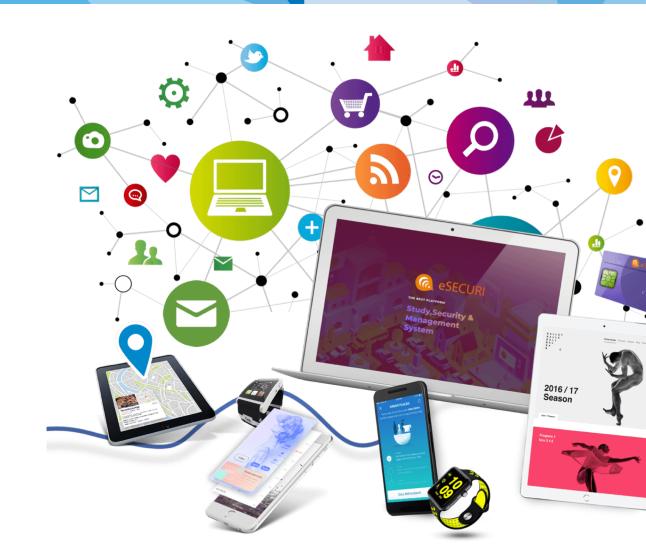
What Personal Information are You collecting?

- Financial information: account numbers
- Drivers License-Government IDs
- Rental Agreements



Where is the Information Stored?

- Laptop, desktop
- Cellphones, tablets
- Cloud
- Vendors/CRM







# Securely Dispose What You Don't Need





### Have a Plan

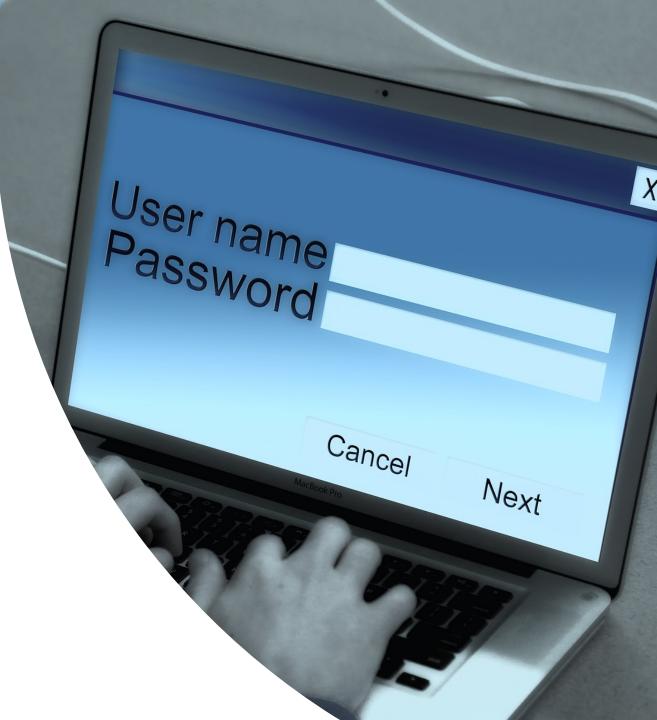
- Create a data security plan
  - Model breach notification document
- Wire fraud communications plan for clients—at each critical point of transaction
- Have a protocol if wire fraud strikes
- Train and retrain

The mine harding and a second to the second

Partic Malari Paskan and Constant and a superior and the second statements and the second statem

## Password Hygiene

- Use a complex password
- Don't share password
- Change your passwords regularly
- Consider a password vault (i.e. Onepassword)



## Surf Smart

- Beware free Wifi
- Use a Virtual Private
  Network
- Keep software updated-security patches current



## **Final Tips**

- NAR has resources to help you
  - Privacy Toolkit
  - Cyber Policy Whitepaper



