# 1 Overview of Cyber Risks

*William and Nancy Skog had cherry-picked an impeccable, perfect, river-front residence in Wilmington, Illinois. Exhilarated by the thought of moving into their dream home, the Skogs could practically see their new lives—watching the tranquil riverboats cruise by and listening to the water birds sing. There was one final step needed to finalize their purchase—wire $307,000 in closing costs to their real estate attorneys. Having received an email with payment instructions sent from what looked like a legal assistant at the firm, William and Nancy wired over their entire life savings—$307,000. Their new life was about to begin. Days later, however, the couple sat across from their lawyer at the closing table and learned their payment never arrived. The Skogs immediately panicked. If their attorneys didn't get the money, who did?*



Let's take a closer look at the details of the wire transfer scam. All $307,000 of the Skogs' hard-earned cash had vanished without a trace. Fraudsters, impersonating their real estate attorneys, had pocketed the entire wire transfer. Almost everything in the closing cost email the Skogs had received looked genuine. The email signatures appeared authentic (because the bad actor copied and pasted the real one), the file attachment had the attorney's actual letterhead, and the details of the real estate transaction were accurate.

How could a bad actor obtain all of this information? A variety of attack methods and vectors could have been used: including compromising one or more email accounts of those involved in the transaction, pretending to be a prospective client and emailing the firm to obtain a response and thus an email signature, or finding the attorneys' letterhead via an Internet search.

Bad actors use automated hacking software that scans data breach dumps for email addresses of people working in a specific industry, such as real estate. Once they collect a list of email addresses, they send *phishing* emails (an email-based, social engineering attack) to obtain the victim's email account password fraudulently. Once they have the password and successfully gain access, they research and monitor real estate transactions in flux. When the timing is right, bad actors send an email to home buyers with "new" wire transfer instructions.[1] It can be easy for victims to believe the malicious email is legitimate, since it can actually be sent from the authentic (hacked) account of one of the real parties involved.

**WARNING** The best method of protection is to not trust email and to be extremely cautious when receiving emails requesting money.

Despite the scam's convincing elements, there were indicators something was wrong. The fraudulent email used unorthodox sentence structure, such as ". . . and have us set ready your closing." Notice anything yet? But beyond suspicious grammar, what could have tipped the Skogs off to the fake email sent by the bad actor? The sender's email address and links might have contained clues. Hovering over any links in the email could have produced red flags, like different or similar-looking URL addresses (for example, `RealEstate.com` versus the malicious URL `RealEstate-co.com`).

Next, the circumstances themselves were reason enough to be wary. Cyberattackers and scammers target their victims in moments of heightened emotion. People are often distracted and/or overwhelmed when scared or elated. In the case of the Skogs, the adversary recognized an opportunity when the Skogs were buying their dream home—a scary and thrilling life event. It was the perfect storm of emotions to render the Skogs vulnerable and allow the scammers to steal the couple's hard-earned life savings successfully when they least expected it. The couple's only saving grace was their daughter, who purchased the home for them.

The Skogs' tremendous loss to real estate wire transfer fraud is indicative of a growing epidemic. In 2016, the FBI found that $19 million in real estate transactions were "diverted or attempted to be diverted" by bad actors, and that amount increased to practically $1 billion in 2017—a 5,163 percent increase in just one year.[2] The cruelest part of real estate wire transfer fraud is the rare chance of ever recovering stolen funds. According to James Barnacle, chief of

the FBI's Money Laundering Unit, "I don't want to set false expectations for consumers. The chance of recovery here is slim."[3]

## Real Estate Wire Transfer Fraud Prevention Steps

Now that you've learned the life-shattering reality of real estate wire transfer fraud, here are some essential prevention steps:

- Before performing a wire transfer, confirm the exact closing instructions with your real estate broker, attorney, or both, in-person, over video or on the phone. (Remember to validate their phone number first.)
- Verify all emails received are genuine. Look out for red flags indicating a phishing email attack, and be suspicious of clicking any email links or opening any file attachments. (You will learn more about phishing email attacks in Chapter 4 and Chapter 5, as well as how to protect your email in Chapter 12.)
- Review other payment options that can potentially provide more protection than a wire transfer, like a cashier's check.
- Initiate a test wire transfer for $100 and confirm the intended receipent received the wire transfer.
- Don't use insecure Wi-Fi to access or send email communications about sensitive transactions. (See Chapter 15 for safe web browsing practices when using public Wi-Fi.)
- Secure your email account with two-factor authentication, and use a strong and unique password for each of your accounts. (See Chapter 15 for details on protecting web access and passwords.)
- Consider using a secure method of file transfer and storage. Use a paid version of Box.com or similar trusted cloud environment. This will allow you to transfer files securely and control which email addresses can access the files.
- Check to see whether your financial institution has insurance available for purchase to protect you from wire transfer fraud liability. Banks are just starting to sell policies for wire transfer fraud protection up to a certain amount. Because there's no standardized, one-size-fits-all policy, check the fine print for variations among banks.[4]

## If You're a Victim of Wire Transfer Fraud

If you've fallen victim to a real estate wire transfer scam, here are immediate incident response recommendations:

- Call the bank that sent the transfer to discuss your options.
- Alert the bank on the receiving end to discuss your options.
- Notify local law enforcement, and file a police report.
- Notify your local FBI field office, and file a complaint.
- Visit the FBI Internet Crime Complaint Center (IC3) and file a complaint online at `https://www.ic3.gov/default.aspx`.

Real estate wire transfer fraud is just one example of the many common and devastating cyber risks we face. Cyberattacks are growing and evolving at a staggering rate, but by continually practicing the handful of basic protection techniques you'll soon learn, you can strengthen your cybersecurity with ease.

## Cyber-Risk Statistics

Serving as a testament to the increase in cyber risk and the need for easy-to-understand, personal, cybersecurity guidance, Verizon published the following statistics in its 2017 "Data Breach Investigations Report," sourced from 65 organizations:[5]

- 51 percent of data breaches involved organized crime groups.
- 1 in 14 people were tricked into clicking a malicious link or email attachment.
- 66 percent of malware was installed by opening malicious email attachments.
- 43 percent of all data breaches used social media attacks.
- 81 percent of hacking-related breaches used stolen and/or weak passwords to gain access.
- 93 percent of social engineering used phishing techniques.
- 14 percent of breaches were caused by mistake.

Why do attackers have such a high success rate in wreaking havoc and causing breaches? One possible explanation is that people rely solely on technology

to protect them. In reality, antivirus and firewalls can only do so much, and they don't provide any protection against "legit" emails from compromised counterparties, such as your lawyer, real estate agent, or banker. It takes individual awareness and implementation of proper cyberhygiene practices to defend oneself holistically.

Throughout the book, you will learn about how to defend yourself against the vast majority of threats. There are a set of fundamentals, which when practiced together will dramatically increase your cybersecurity posture. I simply call this collection of activities and technology "Brilliance in the Basics."

Brian Krebs, a well-known cybersecurity researcher and investigative reporter, put together a "Cybercriminal Code of Ethics," to convey "immutable truths" depicting how bad actors benefit from a lack of investment in personal cybersecurity.[6]

- If you hook it up to the Internet, we'll hack at it.
- If what you put on the Internet is worth anything, one of us is going to try to steal it.
- Even if we can't use what we stole, it's no big deal. There's no hurry to sell it, and we know people.
- We can't promise to get top dollar for what we took from you, but hey—it's a buyer's market. Be glad we didn't just publish it all online.
- If you can't or won't invest a fraction of what your stuff is worth to protect it from the likes of us, don't worry: you're our favorite type of customer!

Another reason cyberattackers are successful is individuals don't necessarily have the proper cybersecurity knowledge to detect cyber threats. (You will obtain that knowledge reading this book!) Scotland Yard found in every month London citizens lose $36 million and report around 3,500 cases of cyber fraud. The most common offenses include phishing emails and malware such as ransomware. Bad actors are aware of this lack of understanding when it comes to cyberattacks. Instead of attempting to compromise a company's firewall directly, these scammers target individuals via their personal lives. The hope is this approach will provide a path to a company's network and thus multiple victims. From here, these bad actors can steal personal information, money, and computing resources.[7]

## Breaches, Cyberattacks, and Hacks—Oh My!

Now you've read a bunch of statistics about breaches, cyberattacks, and hacks—what do they actually mean, and what's the difference between the three?

A *breach* is an incident where sensitive, private, or confidential information is accessed or leaked without authorization. The types of information valued by bad actors include Social Security numbers, credit card and bank account numbers, billing addresses, tax returns, medical information, usernames and passwords, and more.

A breach can be a result from a cyberattack, a hack, or simply a mistake. Each week, bad actors break into networks and systems and steal people's information, sometimes amounting to tens of millions of data elements or more. Most of the time, this stolen data is used to commit fraud. At other times, it can be used as blackmail, such as the case with the Ashley Madison breach, which leaked names and credit card numbers of customers of the extramarital affair website. Bad actors got ahold of the leaked information and threatened Ashley Madison customers into paying a fee; or else they would divulge their activities to their spouses and the general public.

Companies nowadays store massive amounts of personal information about their users for the purposes of its services, ease of access, data analysis, or the convenience of automated payments. Data can be seen as a toxic asset—the more it's accumulated and the longer it sits in storage, the higher the stakes if the information gets into the wrong hands.[8]

A *cyberattack* is when attackers (that is, individuals, criminal organizations, nation states, terrorist organizations, and so on) carry out malicious attacks, such as social engineering against people with the primary objective of accessing, modifying, disclosing, or selling stolen information. Cyberattack targets can include individuals, businesses, government agencies, national infrastructure, and more. A cyberattack doesn't necessarily involve the act of hacking or even the direct use of computers.

A *hack* is a simple or complex act of malicious intent that involves using automated or manual technology to crack a code or break into a target's computer systems or network. It is simply digital trespassing.

Hacking can be a component of a cyberattack, which can lead to a *data breach*, but a cyberattack doesn't necessarily require hacking skills or computers at all. A data breach can occur without a cyberattack or a hack. A data

breach can happen by mistake; as an example, someone sends an email to the wrong person or list of people, resulting in a data breach. Have you ever written an email, attached a sensitive file, and then accidentally sent it to the wrong person? Yep—we've all done it. This is considered a data breach since you didn't intend to send the information to those recipients.

Now that you've read about the main differences between a breach, a cyberattack, and a hack, in the next chapter you will learn who the adversary is, what they want from you, and how you can protect yourself and your family from their cyberattacks and scams.

## Notes

1. https://youtu.be/ToUEr4X1WgU
2. www.chicagotribune.com/classified/realestate/ct-re-1105-kenneth-harney-20171030-story.html
3. https://www.cnbc.com/2017/10/19/scammers-are-conning-home-buyers-out-of-their-down-payment.html
4. http://insurancesidebar.com/Home/tabid/427/entryid/158/Make-Sure-to-Read-Fine-Print-with-New-Wire-Transfer-Fraud-Insurance.aspx
5. www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf
6. https://krebsonsecurity.com/2017/01/krebss-immutable-truths-about-data-breaches/
7. https://www.standard.co.uk/news/crime/cyber-crime-costs-londoners-26-million-a-month-police-warn-a3784706.html
8. https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html