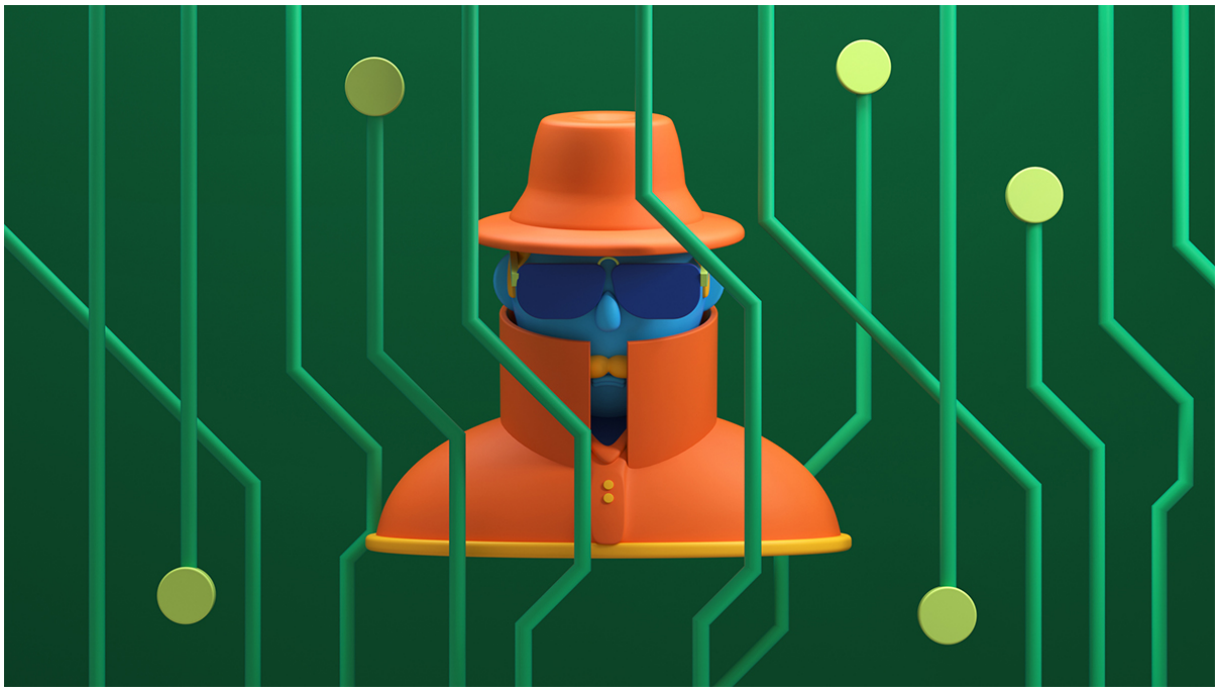
Harvard
Business
Review

Cybersecurity And Digital Privacy

Cyber Thieves Are Getting More Creative

by Stuart Madnick

April 24, 2023



Carlo Cadenas

Summary. Cybercriminals pull off many of their crimes by combining lots of *real* information with just a *tiny bit* of misinformation, which can be financially devastating for both companies and individuals. This article describes some recent examples of this technique, which include exploiting wire transfers, stealing paychecks, and tricking employees into helping "the boss." It's important to continually learn about such new schemes so that you know what to look for and how to prepare your defenses. While there are things that can be done to eliminate

or at least dramatically reduce such crimes, procedures and precautions need to be put in place now, not after a crime has already taken place — especially as cybercriminals themselves get more and more creative. **close**

Misinformation is frequently mentioned in the media, usually in the context of politics and viewed synonymously with fake news. Although these are serious issues, a bigger and more personal danger is often overlooked: How cyber criminals use misinformation to steal from companies and individuals.

One definition of misinformation is: "false or inaccurate information, especially that which is deliberately intended to deceive." But misinformation can be most effective and deceptive when it is combined with large amounts of true and accurate information, especially information that is only known to a few. By exploiting cyberattacks that steal *true* information, criminals can combine that with just a *bit* of misinformation to result in major financial impacts for companies and individuals.

I give several examples below. Because these situations were very sensitive, the organizations affected only agreed to explain the situations to me under the condition of anonymity. This is a common requirement, which is why it is believed that publicly-reported cyberattacks only represent a small fraction of actual cyberattacks.

Exploiting Wire Transfers

Most of us have heard about scams that steal credit card numbers. In most cases, you can challenge or cancel improper credit card charges, so you don't ultimately lose any money. But there's a key difference with wire transfers: they're usually immediate and irreversible. That is, when a wire transfer is used, the money is

gone, especially if this deception is not discovered immediately. Cyber criminals have taken advantage of this feature in various ways.

One example involves criminals getting into a company's computer systems, where they then spend time reading emails and learning internal procedures. The criminals learn which officials are authorized to issue wire transfer instructions to the financial office and what the procedures are. They then masquerade themselves as these officials, one-by-one over several days, issuing instructions for wire transfers, some for more than $500,000, to the criminal's accounts.

After this costly problem was realized at one company I spoke with, procedures were put in place to require verification that such wire transfers were actually requested by authorized personnel. This involved speaking on the phone directly with the authorized person and verifying the details of the transaction. Unfortunately, such sensible procedures are often only put in place *after* a crime has already been committed.

It's not only corporations that can lose money via wire fraud. Executive home buyers are popular targets. A key step in most home buying transactions involves the transfer of a substantial amount of money by wire to a title or escrow company that holds onto the money until the title for the property has been transferred to the new owner and then — and only then — the escrow company transfers those funds to the home seller.

Criminals use a multi-step process to reap their gains in these situations. First, they break into the real estate agent, attorney, or title agent's computer systems. They may spend weeks or even months learning about upcoming closings, the company's procedures, and details including samples of wire transfer instructions. Since there can be complications at the last minute,

home buyers are often encouraged to do the wire transfer a day or two in advance. The title company usually sends the instructions one day in advance, so cyber criminals will send the instructions two days in advance. These instructions appear to be from the title company, since they are based upon the real instructions, but the destination information is altered. They have buried just a bit of misinformation in a batch of true information.

Hundreds of millions of dollars have been stolen this way in a single year. In fact, more than 13,000 people were victims of wire fraud in the real estate and rental sector in 2020, with losses of more than $213 million — an increase of 380% since 2017, according to FBI data. You could find yourself in a situation where you had sold your prior home and used the cash received plus your savings to buy a newer, better home in a different city. You might be in your car halfway to the new city to move into your new home the next day when you receive a call from your real estate agent asking where your payment is. After many frantic calls, you realize that your money has been stolen, and that you're now homeless and broke.

There are various things that both individuals and companies can do to reduce the risk of cyber crime via wire transfer. First, always confirm the wire transfer instructions on the phone with the person who *should* be receiving the money before wiring the money. But, be sure that you can confirm that you are actually talking to the right person — the criminals might have included a phony phone number in the instructions that you received, so always verify the correct number in advance using an official website, or by speaking directly to a known source who can verify the correct information.

Stealing Paychecks

Many companies provide systems that allow employees to maintain and update their personal information, such as home address, telephone, and banking details for direct deposit of their monthly paycheck. Criminals have broken into the accounts of some well-paid employees and, the day before the payment was to be sent, changed the bank details. Then, the day after, they changed the bank details back to normal, so nothing would be noticed to be out of order. They continued this scheme for several months until an executive got a notice of insufficient funds on a check and only then realized that the expected monthly payments had not been received by his bank. (I guess none of these executives were balancing their bank accounts monthly!) This illustrates the importance of checking your bank account frequently enough to detect unusual or erroneous activity, especially to confirm that expected deposits are being made.

Tricking People Into Helping the "Boss"

Most of us of have heard about the classic scam where the CEO of the company asks the CFO to send funds somewhere. If you are not a CEO, you might assume that such scams are not relevant to you, but that is not the case.

One form of this scam, especially popular on university campuses, is for a staff member to receive what appears to be an email from a superior, typically the department head. The staff member is told a story such as, "I just realized that I am going to my nephew's birthday party tonight and I am in meetings all day, so I won't have time to buy a gift. Could you do me a small favor and buy a $100 gift card and email me the numbers on the back?" As one victim lamented: "It was not just coming from one of my colleagues; it came in the name of my department chair." In one

case that I heard of, eight out of 10 faculty in a single department fell for the scam. Once again, it is important to verify that the message is really coming from your boss.

Why It's Important to Be Cautious

The point of all of this is that although misinformation, in the form of fake news, is a problem, combining lots of *real* information with just a *tiny bit* of misinformation can be devastating. The examples above are just some recent examples. As noted, there are things that can be done to eliminate or at least dramatically reduce such crimes, but those procedures and precautions need to be put in place now, not after the crime.

But note, cybercriminals are amazingly creative, and are often armed with lots of information about you. More treacherous schemes may be heading our way, so it is important to continually learn about new schemes, be cautious, and prepare your defenses.

Acknowledgement: The research reported in this article was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.