



Photo by Hernan Pauccara from Pexels

WANTED: YOUR INSIGHTS AND REVIEWS ♥

We're still celebrating our recent accolades from G2.com by asking for your review. Do you love Inspired eLearning Security Awareness Training? Share your experience with us and others!

As a thank you to the first 50 respondents for sharing a detailed, balanced, and complete review, we have a \$10 Visa.com gift card (or equivalent). Consider it a fabulous cup of coffee on us.

We appreciate your partnership and look forward to a great year ahead! Thank you from the entire Inspired eLearning team.

[REVIEW US NOW](#)

8 COMMON NETWORK SECURITY THREATS YOU SHOULD KNOW ABOUT

What Are Network Security Threats?

Whether the goal is money, access, or data, hackers employ various elaborate schemes to take what they want from your business.

Cybersecurity has always been a never-ending battle between security researchers (plus the businesses and individuals they protect) and hackers.

- There are [over 18 million websites](#) infected with malware each week, ready to infect another network.
- The average cost of a data breach is at an all-time high, reaching [\\$4.2 million](#) for the first time in 17 years.
- The global loss to cybercrime in 2020 amounted to [\\$1 trillion](#) and is expected to continue rising.

Fortunately, you can mitigate the threats causing this enormous loss by implementing security policies for your company and making use of the tools created by security researchers to defend against hackers.

Hackers target everything connected to a network. Your servers, laptops, desktops, mobile devices, even your Internet of Things (IoT) devices. Due to the sheer amount of attempts and variations, it might be hard to keep your personal and company data protected.

However, knowing which threats you need to protect against will help create better security policies that will defend your company from most threats.

Here are some of the most common security threats you need to be aware of today.

1. Computer Viruses

A type of malicious software or malware, viruses are one of the most common threats you face. Viruses hide behind files you've downloaded and spread to devices and networks this way. The most likely entry point for viruses are things you've recently downloaded, such as a malicious attachment, executables downloaded from shady websites, or even content shared on [social media](#). It's also possible to spread viruses through malicious URLs.

Viruses can lay dormant on your device and will only launch their attack when you execute the macros it's been hiding in. In other words, the virus will get to work once you open the malicious file that slipped through your antivirus.

They're an active threat that often focuses on interrupting the operation of your devices and network. For example, they might slow down your devices, act as a keylogger so they can steal your passwords, or even take control of your machines.

2. Computer Worms

Although it's the second type of malware on this list, worms aren't talked about very often. Yet, it's one of the most common threats to your network, next to viruses.

Similar to viruses, worms replicate and spread from device to device. However, unlike viruses, worms don't need a host to spread. Viruses need human interaction to activate and spread, but worms can spread through your devices without any help once it's within your device or network. Worms look for a security vulnerability and use that to replicate itself and manipulate your devices.

This makes worms a more dangerous threat than viruses, as they can spread exponentially without you even knowing.

3. Spywares

The last type of malware we mention in this article, spyware is specifically used to get sensitive data. Designed to lay low and stay undetected for as long as possible, spyware is hard to detect and hard to get rid of. The data it targets could be your internet history, login credentials, and even your credit card details.

Besides the three mentioned here, the term malware also covers all sorts of malicious code, including ransomware, fileless malware, bots, and adware.

To start with protecting your devices from malware, get a reliable anti-malware that will detect potentially malicious files and quarantine them before they do any harm. Additionally, educate your employees not to click on suspicious links or attachments so the viruses never had the chance of slipping into your network in the first place.

4. Trojans

Trojans, or trojan horses, are malicious code that hide behind legitimate files to trick users into giving them access to sensitive information. A trojan can't replicate itself, but the damage it yields is big enough that you should be concerned about its presence within your devices.

Trojans are designed to do different things, and there are a lot of types out there, but some common examples include:

- Backdoor trojan
- DDoS trojan
- Infostealer trojan
- Spam trojan
- Gamethief trojan

5. DDoS Attacks

Distributed-denial-of-service attacks (DDoS) is a type of attack that aims to flood a server with traffic, taking the server down and making the website or application unusable to genuine users.

A hacker launching a DDoS attack uses a network of malware-infested devices, or a botnet, to overwhelm a server with requests. These devices, called zombies, are usually infected with malware beforehand so that the perpetrator can order the botnet remotely to attack the server when the time comes.

Unlike the other types of attack, a DDoS attack doesn't aim to breach your network. Instead, DDoS attacks are often used when a hacker wants to take down an app or website for a certain reason, such as cyber warfare, hacktivism, or vandalism.

6. Phishing

Phishing is a type of social engineering technique that hackers use to slip malware into the user's network, trick them into giving sensitive data, or manipulate them into giving money.

It's the method cybercriminals turn to at the beginning of an attack, orchestrated or not. Since they need to find a way to get the malware they'll use for the cybercrime into the target's computer networks, they use one of the most vulnerable points in the system: the users.

Although it often happens via email, phishing also happens through calls, SMS, and other messaging apps. Hackers often use phishing to trick a user into clicking a suspicious link, downloading a suspicious attachment, or going to a fake website to fill in their login information.

In addition to setting up email security systems for your organization, you'll also need to train your users on how to identify phishing emails. It sounds easy enough, but some phishing emails have become so sophisticated that even high-level executives with more than adequate training can still be tricked by an experienced fraudster.

Do regular [training sessions](#) with your employees to remind them of the threats they face and level up their identification skills. Additionally, [phishing simulations](#) will keep your users alert when they're browsing their inboxes.

7. SQL Injection Attacks

SQL, or Structured Query Language, is a coding language programmers use to manage databases. Hackers create malicious code using this language to infiltrate your databases through security vulnerabilities and steal data.

Once attackers get unauthorized access to your database, they can do whatever they want with the database, from just stealing a glance at confidential data, manipulating the databases, or even acquiring administrative access to the database.

Unlike malware, which often uses downloadable files as a host, hackers launching an SQL injection attack make use of SQL commands injected into your data input to affect the execution of predefined commands.

8. Man-in-the-middle (MITM) Attacks

Man-in-the-middle attacks happen when an attacker intercepts the channel of communication between two legitimate parties. These two parties might be between a person with another entity or a person with an application.

Either way, the purpose of this type of cyber attack is usually to either eavesdrop on a conversation or to impersonate one of them.

MITM attacks usually happen in two phases: interception and decryption. In interception, the malicious actor targets a poorly secured network, such as public wifi, and looks for security vulnerabilities that will allow them to interfere with the traffic within that network. Once they manage to intercept the traffic, hackers set up their tools between the two targets so they can eavesdrop on the exchange.

Fortunately, most traffic is secured with encryption, such as SSL/TLS. Cybercriminals would need to decrypt the data before they can peek or manipulate the data.

Cybersecurity Is Always Evolving

Whether you like it or not, cybersecurity is continuously evolving. It's a constant battle between the security analysts who created your defenses and the malicious actors who keep coming up with creative ways to get around these defenses. In the same vein, as hackers develop a new method of attack, security professionals will respond by coming up with a new product to counter these threats.

For example, people used to spring into action without much thought whenever a dubious email asking them to send gift cards to cover an emergency is delivered to their inbox.

However, as targets get smarter and better at security awareness, they've stopped responding to these emails. In the first place, the spam filtering technology has also gotten better, which means it's highly likely that the phishing email never arrived to their inbox either.

Hackers respond by launching spear-phishing attacks instead, or highly personalized phishing emails that might trick even the savviest user. In return, companies are providing regular security awareness training and [anti-phishing simulations](#) to make sure that employees are staying alert when facing their inboxes.

Learn More About Network Security Threats With Inspired eLearning

This back and forth never ends. Unfortunately as a result, security might be demoted to a second priority for some companies. This opens a window of opportunity for hackers, as they can attack your outdated security systems and knowledge with more advanced tools.

In addition to the ones mentioned in this article, there are also various other threats that are even harder to handle, such as Advanced Persistent Threats (APTs), zero-day malware, and insider threats.

Implementing reliable endpoint security tools and robust security policies will help you fight most of these threats. There are various security solutions available to help you too, such as firewalls, encryption, and authentication protocols.

For complete protection, it's also necessary to educate employees about the threats they face daily.

[Regular security awareness training](#) helps you keep up with the current threats you face. Having a regular training program gives you and your employees a guideline on how to protect yourself, even when the threat landscape is changing little by little.

Looking to build a training program that will fit your workforce? Our team can come up with the right mix for your company using our comprehensive training modules.

This article was originally posted by Inspired eLearning. [Read the full article here.](#)

JUSTICE DEPARTMENT APPOINTS FIRST DIRECTOR OF NATIONAL CRYPTOCURRENCY ENFORCEMENT TEAM



The U.S. Department of Justice (DoJ) earlier this week appointed Eun Young Choi to serve as the first Director of the National Cryptocurrency Enforcement Team (NCET) it established last year.

The NCET was [created](#) to tackle the criminal misuse of cryptocurrencies and digital assets," with a focus on illegal activities in virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors to fuel cyberattacks and ransomware and extortion schemes.

"The NCET will serve as the focal point for the department's efforts to tackle the growth of crime involving [digital assets and distributed ledger] technologies," [said](#) Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division.

Separately, the Federal Bureau of Investigation (FBI) said it's [launching](#) a new effort of its own called the Virtual Asset Exploitation Unit (VAXU) dedicated to tracking and seizing illicit cryptocurrencies as part of a broader endeavor to disrupt international criminal networks.

The Justice Department is also setting up a new International Virtual Currency Initiative to allow for international law enforcement operations to trace blockchain money trails as well as develop regulations and anti-money laundering legislation to root out the abuse of cryptocurrency.

The appointment comes as cybercriminals [laundered \\$8.6 billion](#) in cryptocurrencies in 2021, up 30% from 2020, according to blockchain analytics firm Chainalysis. The ill-gotten currencies

account for crypto-native crimes such as darknet market sales or ransomware attacks in which profits are in digital instead of fiat currencies.

Furthermore, 2021 witnessed a marked increase in criminal balances in 2021, with malicious parties [holding \\$11 billion](#) worth of funds with known illicit sources at the end of the year, compared to just \$3 billion at the end of 2020.

On top of that, the North Korean advanced persistent threat (APT) known as Lazarus Group launched at least seven attacks on cryptocurrency platforms that [extracted roughly \\$400 million](#) worth of digital assets in 2021.

That's not all. Russia-linked cybercriminals also set the pace for [ransomware](#) and cryptocurrency-based money laundering activity last year, raking in [nearly 74% of ransom payments](#) in 2021 – over \$400 million worth of cryptocurrency – through strains "highly likely" affiliated with the country.

"The NCET will play a pivotal role in ensuring that as the technology surrounding digital assets grows and evolves, the department in turn accelerates and expands its efforts to combat their illicit abuse by criminals of all kinds," Director Choi said in a statement.

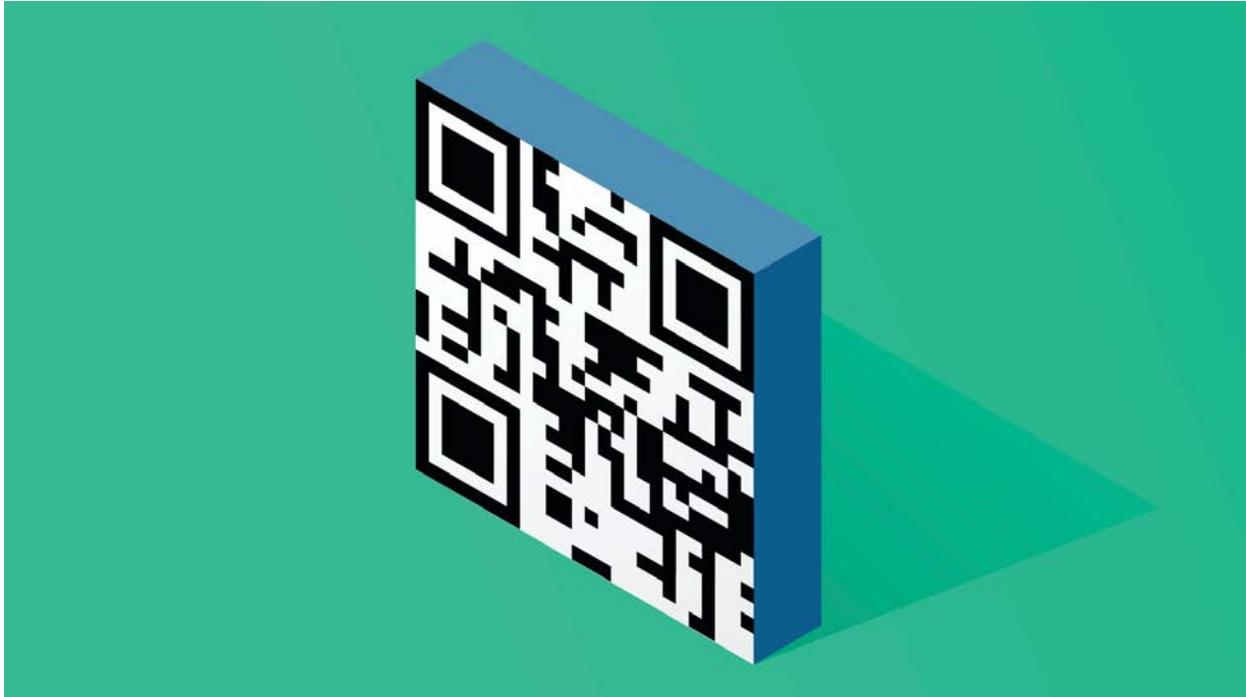
This article was originally posted by The Hacker News. Read the full article [here](#).

IF YOU SCANNED THAT QR CODE FROM THE SUPER BOWL (OR ANY QR CODE), THE FBI HAS A WARNING FOR YOU

QR codes are appearing everywhere--even in Super Bowl ads--but consumers and business owners should know that there are risks. By Jason Aten

The most talked-about ad from the Super Bowl this year was a colorful QR code bouncing around the television screen. If you pointed the camera on your smartphone at it, you were taken to the website for Coinbase, a cryptocurrency exchange. It's a remarkably simple way to generate some viral marketing.

The ad generated so much traffic that it crashed Coinbase's app, which, as I wrote previously, is a bad thing when you're trying to convince people they should trust you with their financial assets. More important, however, is that the QR code seems to finally be making its way to the mainstream.



Getty Images

One of the reasons is Covid-19. QR codes are popping up everywhere as a way to direct customers to information without having to hand them a piece of paper or take a chance that they might mistype a URL.

There's a problem, however. Not every QR code is what it seems, and they've become a tool for bad actors. That's why the FBI is warning consumers to be aware any time they scan a QR code and take steps to protect their information. While the FBI's warning isn't specifically in response to the Coinbase ad, there's an important lesson here--not just for consumers, but for business owners, as well.

The beauty of a QR code is that instead of asking someone to remember a website, you simply embed it in the code. When they scan the code, it takes them directly to whatever webpage you want.

So a restaurant can put its menu online, put a sticker with a QR code on the table, and diners can simply scan the code and view the menu on their phone. As businesses tried to figure out how to safely operate during a pandemic, the idea that you wouldn't have to pass menus back and forth between people was very appealing.

QR codes can also be used to facilitate payments. For example, PayPal and Venmo allow users to scan a QR code to send money to each other. As you might imagine, anytime a new technology makes it easier to get people to visit a website, or send money, someone is going to abuse it. That's exactly the warning that the FBI sent last month:

"Cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use."

Even though the FBI was talking about QR codes generally, Coinbase's ad was probably the most widely-used QR code ever. Millions of people saw the ad, and a large number of them scanned the code.

The problem is: What happens when a bad actor decides to take advantage of the publicity and send out emails with QR codes telling people they can scan it and take advantage of an "offer"? Because a QR code masks the website you are visiting, it's easier to scam someone into handing over their personal information.

If I made a website at the domain `coinbasead.stealyourbitcoin.ru`, you're probably not going to type that into a website. On the other hand, if I embed it in a QR code--and send it out in a convincing email--when you scan it, you'll see "coinbasead" and might not pay much attention to the rest of it. It's not hard to make a copycat website designed only to steal your personal information, or your Bitcoin.

The FBI also warns that "malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location, as well as personal and financial information."

This is less of a concern on an iPhone due to the fact that you can't download software to your device from a web browser on iOS. It doesn't mean, however, that a bad actor can't just create an app that runs directly in the browser. On devices where you can download software directly from the internet, like an Android, QR codes could pose an even bigger threat.

Thankfully, there are a few things you can do to protect yourself when scanning QR codes.

First, only scan a QR code from a trusted source. If you visit a restaurant and your server places a table tent with a code on it so you can view the menu, you're probably fine.

On the other hand, if you walk up to an ATM and there's a sticker next to the screen that says, "Make your transaction online using this code and we'll give you \$50," it's probably a scam. In fact, I personally wouldn't ever scan a QR code on a sticker without first asking, to be sure it's legitimate.

Second, when you scan a QR code, make sure that the website you visit is authentic. Check the URL to make sure it's what you expected. Don't ever enter your personal information on a website without verifying that it is official and secure.

Also, if you get an email with a QR code, there's no reason to ever scan it. QR codes are meant for interactions where you can't just click on a link. If the person sending you an email doesn't include the link in the body of the email, that should be a red flag.

Finally, if you're a business and you are using QR codes, there are a couple of things you should do as well. If you're going to use a QR code, make sure that the one your customers scan is the one you created. That means making sure no one has covered the official code with a sticker, for example.

Also, including the URL on your sign can help customers have peace of mind when scanning your code. Include language along the lines of, "This code will take you to our menu at menu.reallynicerestaurant.com. If it doesn't, please let us know, and don't enter any personal information."

This article was originally posted by Inc.com. Read the full article [here](#).

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning's parent organization, VIPRE Security Group, is doing to better our product experience for our customers.

Vulnerability and Patch Management Add-On
Now Available for VIPRE Endpoint Security Cloud

[LEARN MORE](#)

VIPRE Email Link Isolation Just Released

[LEARN MORE](#)



CONNECT WITH US

© 2022 Inspired eLearning, LLC.

All rights reserved.

info@inspiredelearning.com | 800.631.2078