ĀURA

Protecting Consumers from Evolving Digital Threats

Cybercriminals are more sophisticated than ever and consumers are at risk

This past year, financial losses as a result of digital crime surpassed those of home bulgarlies for the first time, according to data from the Federal Bureau of Investigation (FBI)'s Preliminary 2020 Crime Report and the Federal Trade Commission (FTC)'s 2020 Consumer Sentinel Report. But cybercrime attacks aren't just becoming more common - they are growing in sophistication in an attempt to combat new technology that can better detect and prevent threats.

The typical consumer today has an average of 90 online accounts and spends almost seven hours online each day, and most (80%) **U.S. adults say they should be doing more to protect their personal information**, according to a survey by Harris Poll and digital security company Aura.

But despite this, the same group surveyed continues to use public wifi (68%) and the same password for multiple accounts (68%), behaviors that make it easier for cybercriminals to gain access to data they ultimately use to finetune attacks.

Survey respondents may know they can - and should - change their online behaviors to reduce their risk of cybercrime, but most haven't because it's too time consuming (36%), aren't sure how (33%), or find it too difficult (17%).

This piece seeks to address this disconnect by highlighting common digital threats, as well as steps consumers can take to better protect themselves online.

Protecting Yourself from Cybercrime: Social Engineering

Social engineering is perhaps the most important cybercrime tactic to understand, given it is a common foundation for many forms of threats. This tactic exploits human nature, rather than technical expertise or hacking, to gain access to information, data, finances, systems and more. Criminals typically research social media and other publicly available information to impersonate someone or something, aiming to gain the victim's trust.

Examples

- A criminal might enter an office building behind you, saying they've forgotten their key card or have their hands full, while wearing a company t-shirt they purchased online.
- They may pose as law enforcement over the phone or call an employer claiming they've been locked out of their account. They could "verify" their identity by correctly guessing the email address of the person they claim to be after seeing the first.last@company.com format posted in a press release or on the website.

Protect against social engineering

- → Check the source - and take a moment to consider whether you should trust it. It's very unlikely that your CEO would ask you to transfer a large sum of money, for example.
- → Consider if the source has the information they reasonably should, like your full name, your security questions, or home address.
- → Go to the source directly - hang up and call the phone number on your last invoice or the source's official website.
- → Ask for identification or to speak with a supervisor.

Protecting Yourself from Cybercrime: Phishing/vishing/smishing

Phishing attacks are fraudulent communications that appear to come from a reputable source, often via email (phishing), phone (vishing) or text (smishing). They typically attempt to instill fear or urgency, or take advantage of the victim's curiosity or greed.

Example

Phishing attacks often offer too-good-to-be-true deals, urgent notification to reset an account login because of suspicious activity, or contain an attachment or hyperlinks they want the victim to open. The goal may be to install malware, steal credit card data or access login information.

Protect against phishing

- Hover over links before clicking them. Check that the URL makes sense - look for a letter or number that is off.
- Visit the perceived sender's website or contact them directly to confirm the message's legitimacy.
- Do not download or open emails you weren't expecting or from senders who aren't in your typical email list. For example, if you subscribe to retailer offers with a personal email, but receive a promotion to your business email address, be suspicious.
- Never give out personal, sensitive information via email.
- Be cautious of emotional and urgent lures.

Protecting Yourself from Cybercrime: Malware

Malware is an umbrella term for malicious software designed to harm a device, network or service, such as a virus.

Examples

Scareware, for example, is a malware tactic that exploits a user's fear and leads them to believe they need to download or buy something (e.g. antivirus software) that is actually harmful, like ransomware.

Ransomware is a form of malware that uses encryption to hold a victim's information, data or files at ransom. The attacker demands a ransom to deliver a decryption key that will (usually) restore access to the files or data. These attacks are often made possible through phishing or social engineering, with the attacker, for example, posing as law enforcement, claiming they found illegal data or images on the victim's device, and asserting they will not reinstate access until a fine is paid. The criminal may also threaten to leak embarrassing, proprietary or valuable data or information if the ransom isn't paid.

Other forms of malware include but are not limited to adware (displays advertisements on your screen while collecting personal information to serve you with more personalized ads), spyware (invades your device in an attempt to steal credit card or banking information, passwords or other data), trojans (camouflages as legitimate software to trick you into installing harmful software), rootkits (enable unauthorized use of your device), rootware (replicates itself to infect other devices connected to a network) and more.

Protect against malware

- Stay vigilant against phishing attempts.
- Keep your operating system, antivirus software and device up to date.
- Don't use an unknown USB stick.
- Back up files and information to minimize potential damage.
- Avoid downloads from sites you don't trust.
- Don't install software unless you know what it's for or who/where it came from.
- Avoid public wifi or use VPN when on a public or shared network.

Protecting Yourself from Cybercrime: Imposter Scams

Most consumers have probably experienced an **imposter scam**, also rooted in social engineering tactics. These types of cyberattacks often begin with a call, text or email, and while the scam itself varies, they all work the same way - with an impersonator of someone you trust asking for money or personal information.

Examples

- Calls from the "Internal Revenue Service (IRS)" claiming you owe taxes
- Callers claiming to be the Social Security Administration, saying there's a warrant out for your arrest
- Someone you met on the internet or an online dating site asks for money
- Calls from a someone pretending to be a child or grandchild, saying they're in trouble and need money
- Calls from "tech support" claiming to help fix your computer
- A fake employer on caregiver or nanny sites, asking you to purchase supplies for your job after sending a large check (that will bounce

Protect against imposter scams

- → Be suspicious of calls from any government agency. The FTC has issued warnings around this type of attack, and they will not use threats or demand money.
- → Don't trust caller ID - it's possible to fake.
- → Don't pay with a gift card, wire transfer or cryptocurrency over the phone or via text.
- → Confirm the source of the inquiry directly by using a phone number you've looked up and dialed yourself.
- → Don't install software unless you know what it's for or who/where it came from.

Protecting Yourself from Cybercrime: Online Shopping Scams

Online shopping scams are another growing form of cybercrime. According to the FBI, these scams direct victims to fraudulent websites via ads on social media platforms and popular online search engines' shopping pages, and could result in undisclosed costs to the user, failure to deliver products on time (if at all), refusals to honor guarantees made or preventing negative reviews. Often these sites offer a product at an extremely low price, and while some victims receive partial reimbursement, most don't. In fact, according to a 2020 FBI Public Service Announcement, all attempts made by victims to be fully reimbursed by online shopping scams, or to receive the actual items ordered, were unsuccessful.

Examples

- When browsing social media, sponsored content pops up, promoting a product you're interested in purchasing. However, after you purchase the item, you never receive your order and aren't able to reach anyone at the "retailer" or find a confirmation email.
- You might use an online marketplace to buy a product that has excellent reviews and is being sold at the lowest price. But after receiving your order, you realize the product is not the quality level suggested on the website, begin a return and write a bad review. The "retailer" then reaches out saying that your return will not be completed unless you delete your negative review.

Protect against online shopping scams

- → Be suspicious of calls from any government agency. The FTC has issued warnings around this type of attack, and they will not use threats or demand money.
- → Don't trust caller ID - it's possible to fake.
- → Don't pay with a gift card, wire transfer or cryptocurrency over the phone or via text.
- → Confirm the source of the inquiry directly by using a phone number you've looked up and dialed yourself.
- → Don't install software unless you know what it's for or who/where it came from.

Protecting Yourself from Cybercrime: Man-in-the-Middle Attacks

In the case of a **man-in-the-middle** (MITM) attack, a cybercriminal typically gains access to an unsecured or public wifi server. Once they've gotten inside, the attacker might be a passive listener, capturing sensitive personal information like credit card data, bank account or login credentials. Or, they may be an active participant, changing your messages or impersonating someone you're talking to.

Examples

- An attacker might snoop at a coffee shop through the public wifi, and once they've gotten in, they watch you enter your username and password to an online account. They might use this information to try to gain access to your bank account or professional account for a larger scale attack against your employer.
- A criminal may gain access to your activity through shared airport wifi, and watch as you enter your credit card information on a shopping site or impersonate someone you're chatting with to gain access to this information.

Protect against Man-in-the-middle attacks

- → Don't connect to public or shared wifi networks.
- → Use a virtual private network (VPN).
- → Install security solutions on your devices.
- → Secure your home wifi network with a strong password.
- → Be sensitive to unexpected or repeated disconnection.

Protecting Yourself from Cybercrime: Identity Theft

Of all the types of fraud consumers reported to the FTC in 2020, **identity theft** was the most common. Identity theft occurs when a criminal steals your personal information to commit fraud, such as applying for credit, filing taxes, or accessing medical care. With only a social security number (SSN), cybercriminals can secure a loan or credit card in the victim's name, drain their bank account, use their health insurance, claim Social Security, and even identify themselves as the victim to police in the event of an arrest.

Examples

- Tax - Using your SSN to file fake tax returns
- Medical - Using your health insurance number to get medical services or send fake bills to your health insurer for reimbursement
- Unemployment - Using your information to access unemployment - or other types of government - benefits

Protect against identity theft

- Be protective of your SSN. Don't write it down unless you watch the recipient shred it after. Don't share your SSN out loud when others are around. Don't carry your Social Security card in your wallet.
- Be protective of your other sensitive, personal information, like birthdate, bank account number, address, etc., as they can all be used to commit identity theft.
- Collect your mail everyday and set up mail forwarding or holding when you will be away.
- Monitor your credit score, bank and financial statements, and take action quickly if anything seems incorrect or suspicious. Shred account statements or other documents with sensitive numbers or information printed on them.
- Freeze your credit for free with any of the three credit bureaus.

Additional suggestions for securing your digital life

Use strong passwords.

Passwords and pins are used by an infinite number of websites and accounts as the first barrier to entry with most, making strong passwords incredibly important. However, roughly 65% of people reuse passwords across sites. Consider these tips when thinking about password practices:

1. The more complex the password (multiple digits/letters, with special characters such as @, # and %, etc.), the more secure. Don't use a pet's name, a hometown or a favorite sports team - or anything a stranger could figure out by looking at your social media history or other publicly available information.

2. Do not use the same password for multiple accounts.Should a criminal successfully breach just one account, they will then attempt to use those credentials to attempt to access the victim's other accounts.

3. Do not write a password down digitally or on paper. If you can't remember your passwords, explore a password manager, which manages different, complex passwords for each account a consumer has across mobile and desktop devices. However, make sure to create a complex password to access the password manager itself, as that will serve as the gatekeeper for all of your other passwords.

Use credit, not debit cards.

Perhaps the single most effective way to protect your finances digitally is giving up your debit card entirely. The benefits of paying with a credit card have nothing to do with the card's security defenses - but rather what happens to the user when a breach happens. Thanks to Zero Liability policies created by banks many years ago to encourage shopping online, resolving issues of credit fraud are often painless. In the instance of fraudulent charges, the bank issuing the card will typically provide the customer an immediate, temporary credit for the fraudulent charge, cancel the card itself and issue a new card immediately. Then, a month or so later, that temporary credit usually becomes permanent. This process means the user can proceed making charges regardless of fraud.

With a debit card, however, this scenario is different. A debit card accesses cash directly from a bank account, meaning a successful debit card attack will often wipe out the user's entire bank account. Most banks, if they verify that a charge was indeed fraud, will replace the money, but that process can take months. In the meantime, any transactions made before the fraud that had not already cleared will fail, and most businesses will charge the fraud victim a penalty - that they may no longer be able to afford - as a result.

Install protective software and keep your device updated.

Use antivirus software, anti-spyware and a firewall on your computer. Be sure to install your computer's updates quickly - or automatically if possible.

Shred documents with sensitive information.

Whenever possible, don't leave behind documents with personal information. In the event of a move or relocation, set up mail forwarding so that credit card offers and other sensitive data reach only you and your family.

Explore fraud alerts.

In the case of a lost wallet, for example, you might be suspicious that identity theft will occur - even if it hasn't, yet. Contact one of the three credit bureaus and ask them to set up a free fraud alert - the bureau you contact will notify the two others.

Freeze your credit.

While it can be inconvenient to freeze your credit, this is a great way to prevent identity thieves from opening new lines of credit using your SSN. Given that nearly 30% of those experiencing identity crime are repeat victims, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, this is especially recommended for past victims. You can contact any of the three credit bureaus and do this for free, and similar to the process with fraud alerts, the one you contact will notify the two other bureaus.

VPN is essential.

Virtual private networks (VPNs) have been used in corporate environments for decades. Today, however, they are essential for consumers to protect communications, whether on a desktop, laptop or a mobile device.

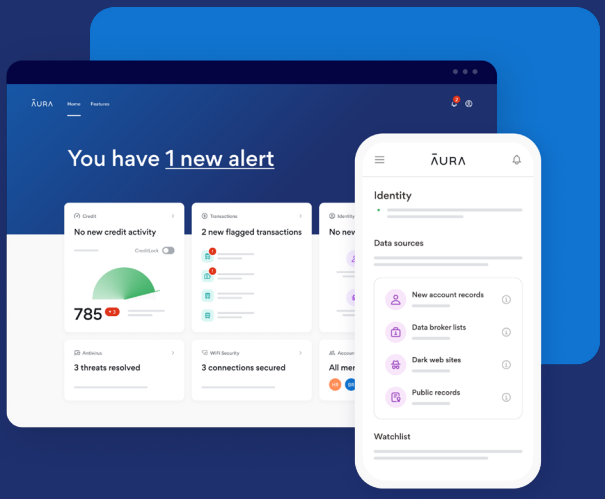
VPNs provide a secure encrypted tunnel between the user's device and a web server or an email host. While a VPN does not protect the data on the user's device, nor that at the recipient's end, it protects data while in transit, which is when most cybercriminals steal sensitive data.

VPNs also deliver a layer of privacy by hiding where the user is located. For example, many VPNs allow the user to choose the geography in which they will appear, whether that is another country, state or a city. Location ambiguity not only makes it more difficult to connect an individual to their unique and specific online profile, but can also help users avoid geographic restrictions on content that would otherwise be unavailable to them.

Explore an all-in-one digital security solution.

At Aura, we understand firsthand how daunting it can be to take control of your digital life. That's why we created easy-to-use, all-in-one digital security protection to keep you and your family's personal information, devices, and finances safe from online threats.

It combines everything you need to proactively control your digital lives - credit monitoring, lost wallet recovery, antivirus, VPN, multi-device protection, and monitors financial transactions, bank accounts, SSN, the dark web, home and title use, and criminal and court records to keep your finances and your identity safe and secure. And in the event of an issue, Aura's U.S.-based customer service team is available to help you resolve problems 24/7. This is all backed by a $1 million dollar identity theft insurance policy for eligible losses for every Aura customer.



The New Standard In Digital Security

media@aura.com aura.com 833.552.2123