

SECURITY AWARENESS



Table of Contents

- Security Awareness Program 3
 - Cybersecurity Education Dashboard 4
- NCSAM 2019 5
 - National Cybersecurity Awareness Month! 6
 - Cybersecurity Awareness Quiz 8
 - 5 Ways to be Cyber Secure at Work..... 10
 - Phishing..... 12
 - Password Best Practices..... 15
 - 5 Steps to Protecting Your Digital Home..... 18
 - Social Media Cybersecurity..... 20
 - Online Privacy 23
 - Identity Theft and Internet Scams..... 26
 - Cybersecurity Awareness Promo 29
 - Cybersecurity While Traveling 30

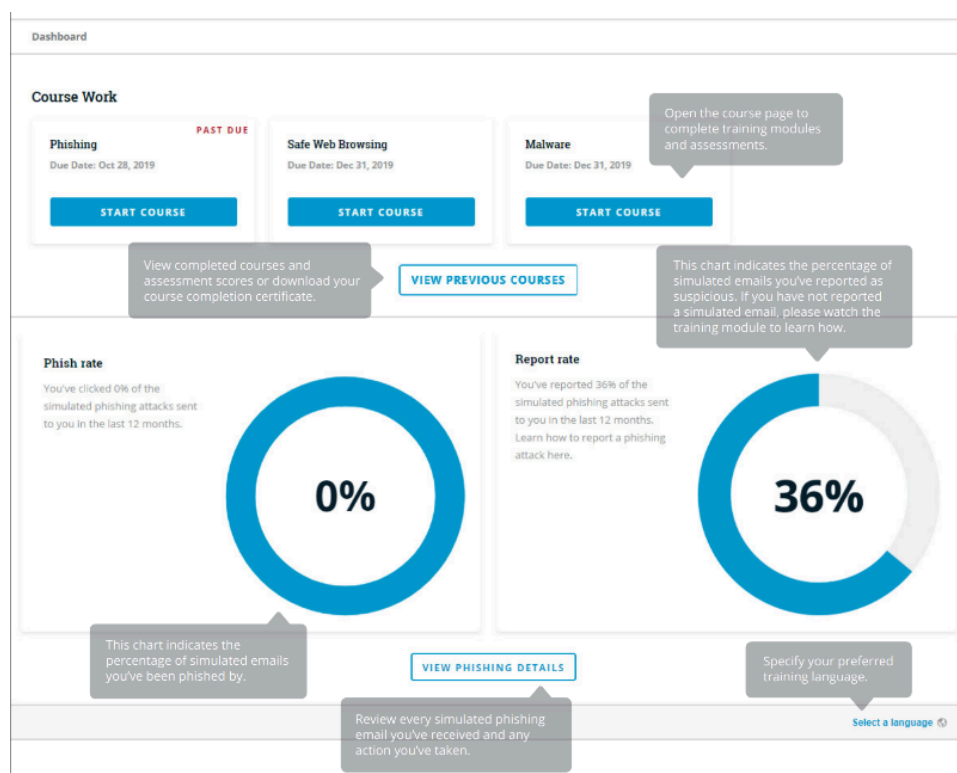
Security Awareness Program

Cybersecurity Education Dashboard

The new dashboard allows you to keep tabs on your cybersecurity training and performance history from your personalized dashboard.

Click your training notification link (sent every few days) to access your personalized dashboard.

From here, you can complete training courses, view completed assignments, review your simulated phishing results and compare your performance with your coworkers.



NCSAM 2019

National Cybersecurity Awareness Month!



Held every October, National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online.

(SOURCE: <https://www.dhs.gov/national-cyber-security-awareness-month>)

Today, Cyber Security's weakest link is the user. Hackers are like vampires they cannot come into your home unless invited in. Hackers will do anything and everything possible to trick a user into letting them in. They'll portray themselves as an authority emailing users as their boss, the police, FBI, or owner of the company. They'll use intimidation do this or else! They'll use familiarity as a tactic, mentioning work colleagues, demonstrating insight into the operation to help build credibility. They'll try many different ways to exploit bad practices at any company.

You may be thinking, 'I'm a small company, I'm not a target', and you'd be wrong. According to Forbes, 58% of cyberattack victims are small businesses. Another study revealed 55% of small businesses have experienced at least one cyberattack within the last 12 months, and nearly a ¼ of those will go out of business because of it. It's not a matter of if you'll suffer a cyberattack, it's when.

(SOURCE: <https://www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#12687eb11953>)

The easiest and most important step to protecting your business from cyberattack is educating your users. This month Fluid Networks is offering a free Security Risk Assessment and Security Awareness Analysis. Take advantage of this special offer to gain an important and real

understanding of your organization's risk and exposure. Too much is at stake to ignore this opportunity!

To take advantage of this promotion please visit our [Cybersecurity Awareness Promo page](#).

For more information as well as insight into the Cyber Security Awareness Contests we're running this month, please visit our [Cybersecurity Awareness Quiz page](#).

Your security and protection is our greatest priority!

Damian C. Stalls
vCIO Director



80 Wood Road, #308
Camarillo, CA 93010
805.856.1806 Support
805.856.1815 Direct
www.fluidnets.com

Follow Us:



Cybersecurity Awareness Quiz



For National Cybersecurity Awareness Month we want to encourage all of our users to be safe when online. During the month of October we will have a new quiz available each week for users to complete. Each user who completes a quiz will be entered into a drawing to win a \$50 Amazon gift card. Any users who get a perfect score on all (4) quizzes will also be entered into a drawing for a \$100 Fry's Electronics gift card.

Follow us on Social media as there will be new #CyberSafe tips posted daily as well as updates on when each quiz is available.



Cyber Security Quiz Links

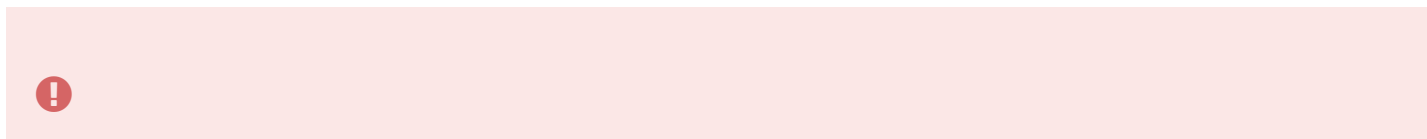
[Online Safety Quiz \(now available\)](#)

[Device Security Quiz \(now available\)](#)

[Types of Cyber Attacks Quiz \(now available\)](#)

[Cyber History Quiz \(now available\)](#)

Drawing Rules



1. The Cyber Security Quiz Drawings are open to people aged 18 and over who provide their email address during the quiz.
2. Employees or agencies of Fluid Networks and their family members may not participate in the Cyber Security Quiz Drawing.
3. Entrants into the Cyber Security Quiz Drawing shall be deemed to have accepted these Terms and Conditions.
4. To enter the Cyber Security Quiz (Amazon gift card) you must complete at least (1) Cyber Security Quiz. To enter the Cyber Security Quiz (Fry's gift card) you must score 100 points on all (4) Cyber Security Quizzes. No purchase is necessary.
5. Only one entry per person, per quiz (If you complete all (4) quizzes you will increase your chances of winning the Amazon gift card).
6. Entries on behalf of another person will not be accepted and joint submissions are not allowed.
7. Fluid Networks accepts no responsibility is taken for entries that are lost, delayed, misdirected or incomplete or cannot be delivered or entered for any technical or other reason. Proof of delivery of the entry is not proof of receipt by Fluid Networks.
8. The closing date of the Cyber Security Quiz Drawing is 11:59pm on November 8, 2019. Quizzes completed outside this time period will not be considered.
9. (4) Amazon gift card winners and (1) Fry's gift card winners will be chosen from a random draw of entries received in accordance with these Terms and Conditions. The drawing will take place on November 12, 2019.
10. Fluid Networks accepts no responsibility for any costs associated with the prize and not specifically included in the prize.
11. The winner will be notified by email on or before November 22, 2019. If a winner rejects their prize or the entry is invalid or in breach of these Terms and Conditions, the winner's prize will be forfeited and Fluid Networks shall be entitled to select another winner.

5 Ways to be Cyber Secure at Work



Businesses face significant financial loss when a cyber attack occurs. In 2018, the U.S. business sector had the largest number of data breaches ever recorded: 571 breaches.¹ Cybercriminals often rely on human error—employees failing to install software patches or clicking on malicious links—to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of everyone to keep data, customers, and capital safe and secure. #BeCyberSmart to connect with confidence and support a culture of cybersecurity at your organization.

SIMPLE TIPS TO SECURE IT.

Treat business information as personal information.

Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information (PII) through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.

Technology has its limits.

As “smart” or data-driven technology evolves, it is important to remember that security measures only work if used correctly by employees. Smart technology runs on data, meaning devices such as smart phones, laptop computers, wireless printers, and other devices are constantly exchanging data to complete tasks. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches. For more information about smart technology see the Internet of Things Tip Card. Read the Internet of Things Tip Sheet for more information.

Be up to date.

Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.

Social media is part of the fraud toolset.

By searching Google and scanning your organization's social media sites, cybercriminals can gather information about your partners and vendors, as well as human resources and financial departments. Employees should avoid over sharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms. Read the Social Media Cybersecurity Tip Sheet for more information.

It only takes one time.

Data breaches do not typically happen when a cybercriminal has hacked into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages immediately. For more information about email and phishing scams see the Phishing Tip Sheet.

References

1. Identity Theft Resource Center, "[2018 End-of-Year Data Breach Report](#)", 2018

Phishing



Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

HOW CRIMINALS LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."
- To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit "

SIMPLE TIPS TO SECURE IT.

Play hard to get with strangers.

Links in email and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.

Think before you act.

Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks "phishy," reach out to them via customer service to verify the communication.

Protect your personal information.

If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

Be wary of hyperlinks.

Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smart phone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

Shake up your password protocol.

According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts. Read the Creating a Password Tip Sheet for more information.

Install and update anti-virus software.

Make sure all of your computers, Internet of Things devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

Password Best Practices



Creating a strong password is an essential step to protecting yourself online. Using long and complex passwords is one of the easiest ways to defend yourself from cybercrime. No citizen is immune to cyber risk, but #BeCyberSmart and you can minimize your chances of an incident.

Simple Tips for a Secure Password

Creating a strong password is easier than you think. Follow these simple tips to shake up your password protocol:

Use a long passphrase

According to NIST guidance, you should consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.

Don't make passwords easy to guess

Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.

Avoid using common words in your password

Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L."

Get creative

Use phonetic replacements, such as “PH” instead of “F”. Or make deliberate, but obvious misspellings, such as “enjin” instead of “engine.”

Keep your passwords on the down-low

Don’t tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.

Unique account, unique password

Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. It’s important to mix things up—find easy-to remember ways to customize your standard password for different sites.


Double your login protection

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smart phone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.

 We have recently partnered with DUO for MFA security. Let us know if you would like information on pricing and how to setup for your company.

Utilize a password manager to remember all your long passwords

The most secure way to store all of your unique passwords is by using a password manager. With just one master password, a computer can generate and retrieve passwords for every account that you have – protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions, and more.

 We recommend using either LastPass or Dashlane to secure your passwords. We can also provide this service as well using our [MyGlue](#) platform. Customers with an AISP Support Agreement can use MyGlue at no additional charge. Talk to your account manager today!

5 Steps to Protecting Your Digital Home



More and more of our home devices—including thermostats, door locks, coffee machines, and smoke alarms—are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which in turn can save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing, however they also pose a new set of security risks. #BeCyberSmart to connect with confidence and protect your digital home

SIMPLE TIPS TO PROTECT IT.

Secure your Wi-Fi network.

Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

If you connect, you must protect.

Whether it's your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you're putting something into your device, such as a USB for an external hard drive, make sure your device's security software scans for viruses and malware. Finally, protect your devices with antivirus software and be sure to periodically back up any data that cannot be recreated such as photos or personal documents.

Keep tabs on your apps.

Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the “rule of least privilege” to delete what you don't need or no longer use. Learn to just say “no” to privilege requests that don't make sense. Only download apps from trusted vendors and sources.

Never click and tell.

Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are— and where you aren't—at any given time

Social Media Cybersecurity



Now more than ever, consumers spend increasing amounts of time on the Internet. With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world. How can you be proactive to stay safe online and, “Own IT. Secure IT. Protect IT.”? #BeCyberSmart and take these simple steps to connect with confidence and safely navigate the social media world.

DID YOU KNOW?

- 3.48 billion people worldwide now use social media worldwide. That’s an increase of 9% from 2018. Put another way: 45% of the total world population are using social networks.(1)
- Digital consumers spend nearly 2.5 hours on social networks and social messaging every day.(2)
- 69% of U.S. adults use at least one social media site(3) and the average American has 7.1 social media accounts.(4)

SIMPLE TIPS TO OWN IT.

Remember, there is no ‘Delete’ button on the Internet.

Share with care, because even if you delete a post or picture from your profile seconds after posting it, chances are someone still saw it.

Update your privacy settings.

Set the privacy and security settings to your comfort level for information sharing. Disable geotagging, which allows anyone to see where you are—and where you aren't—at any given time

Connect only with people you trust.

While some social networks might seem safer for connecting because of the limited personal information shared through them, keep your connections to people you know and trust.

Never click and tell.

Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren't—at any given time.

Speak up if you're uncomfortable.

If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let him or her know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them, and it is important to respect those differences. Don't hesitate to report any instance of cyberbullying you see.

Report suspicious or harassing activity.

Work with your social media platform to report and possibly block harassing users. Report an incident if you've been a victim of cybercrime. Local and national authorities are ready to assist you.

References

1. Kemp, Simon. "Digital 2019: Global Digital Overview." DataReportal. January 30, 2019. <https://datareportal.com/reports/digital-2019-global-digital-overview>.
2. Gwi. "Latest 2019 Social Media User Trends Report." GlobalWebIndex. 2019. <https://www.globalwebindex.com/reports/social>.
3. Newberry, Christina. "130 Social Media Statistics That Matter to Marketers in 2019." Hootsuite Social Media Management. March 13, 2019. <https://blog.hootsuite.com/social-media-statisticsfor-social-media-managers/>.
4. Ibid.

Online Privacy



The Internet touches almost all aspects of our daily lives. We are able to shop, bank, connect with family and friends, and handle our medical records all online. These activities require you to provide personally identifiable information (PII) such as your name, date of birth, account numbers, passwords, and location information. #BeCyberSmart when sharing personal information online to reduce the risk of becoming a cybercrimes victim.

DID YOU KNOW?

- 64% of U.S. adults have noticed or been notified of a major data breach affecting their sensitive accounts or personal data.(1)
- Roughly half of Americans (49%) feel that their personal information is less secure than it was five years ago.(2)
- 58% of Americans age 50 and older are more likely to feel that their personal information has become less safe in recent years: 58% of Americans in this age group express this opinion.(2)
- 69% of consumers believe companies are vulnerable to hacks and cyberattacks.(3)

SIMPLE TIPS TO OWN IT.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

Shake up your password protocol.

According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.

Be up to date.

Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.

If you connect, you must protect.

Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software.

Play hard to get with strangers.

Cyber criminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate—or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender.

Never click and tell.

Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren't—at any given time.

Keep tabs on your apps.

Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the “rule of least privilege” to delete what you don’t need or no longer use. Learn to just say “no” to privilege requests that don’t make sense. Only download apps from trusted vendors and sources.

Stay protected while connected.

Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with “https://” when online shopping or banking.

References

1. Smith, Aaron. “Americans and Cybersecurity.” Pew Research Center: Internet, Science & Tech. April 27, 2017. <https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>.
2. Ibid.
3. PricewaterhouseCoopers. “Consumer Intelligence Series: Protect.me.” PwC. 2017. <https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html>.

Identity Theft and Internet Scams



Today's technology allows us to connect around the world, to bank and shop online, and to control our televisions, homes, and cars from our smartphones. With this added convenience comes an increased risk of identity theft and Internet scams. #BeCyberSmart on the Internet—at home, at school, at work, on mobile devices, and on the go.

DID YOU KNOW?

- The total number of data breaches reported in 2018 decreased 23% from the total number of breaches reported in 2017, but the reported number of consumer records containing sensitive personally identifiable information (PII) exposed increased 126%.(1)
- Credit card fraud tops the list of identity theft reports in 2018. The Federal Trade Commission (FTC) received more than 167,000 reports from people who said their information was misused on an existing account or to open a new credit card account.(2)
- Consumers reported \$905 million in total fraud losses in 2017, a 21.6% increase over 2016.(3)

COMMON INTERNET SCAMS

As technology continues to evolve, cybercriminals will use more sophisticated techniques to exploit technology to steal your identity, personal information, and money. To protect yourself from online threats, you must know what to look for. According to the FTC, these are the top three kinds of threats reported in 2018:

- **Identity theft** is the illegal acquisition and use of someone else's personal information to obtain money or credit. Signs of identity theft include bills for products or services you did not purchase, suspicious charges on your credit cards, or new accounts opened in your name that you did not authorize.

- **Imposter scams** occur when you receive an email or call from a person claiming to be a government official, family member, or friend requesting personal or financial information. For example, an imposter may contact you from the Social Security Administration informing you that your Social Security number (SSN) has been suspended, in hopes you will reveal your SSN or pay to have it reactivated.
- **Debt Collection scams** occur when criminals attempt to collect on a fraudulent debt. Signs the “debt collector” may be a scammer are requests to be paid by wire transfers or credit cards. In 2018 there was a spike in requests for gift cards and reloadable cards as well.

SIMPLE TIPS TO PROTECT IT.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

Shake up your password protocol.

According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.

Be up to date.

Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don’t have to think about it, and set your security software to run regular scans.

PROTECT YOURSELF FROM ONLINE FRAUD

Stay Protected While Connected: The bottom line is that whenever you’re online, you’re vulnerable. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.


- Practice safe web surfing wherever you are by checking for the “green lock” or padlock icon in your browser bar—this signifies a secure connection.

- When you find yourself out in the great “wild Wi-Fi West,” avoid free Internet access with no encryption.
- If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.
- Don’t reveal personally identifiable information such as your bank account number, SSN, or date of birth to unknown sources.
- Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email

RESOURCES AVAILABLE TO YOU

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. The list below outlines the government organizations that you can file a complaint with if you are a victim of cybercrime.

- **FTC.gov:** The FTC’s free, one-stop resource, www.IdentityTheft.gov can help you report and recover from identity theft. Report fraud to the FTC at ftc.gov/OnGuardOnline or ftc.gov/complaint
- **US-CERT.gov:** Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov. Forward phishing emails or websites to US-CERT at phishing-report@us-cert.gov.
- **IC3.gov:** If you are a victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3) at <http://www.IC3.gov>.
- **SSA.gov:** If you believe someone is using your SSN, contact the Social Security Administration’s fraud hotline at 1-800-269-0271.

 Are you a Fluid Networks AISP or MSP customer? If so we can help you gather this information to report the incident to the applicable authorities. Just contact our Helpdesk at (805) 856-1806.

References

1. Identity Theft Resource Center, “[2018 End-of-Year Data Breach Report](#)”, 2018.
2. Federal Trade Commission, “[Consumer Sentinel Network Data Book 2018](#)”, 2019.
3. Experian, “[Identify Theft Statistics](#)”, 2019.

Cybersecurity Awareness Promo



The easiest and most important step to protecting your business from cyberattack is educating your users. This month Fluid Networks is offering a free Security Risk Assessment and Security Awareness Analysis.

If you are an authorized representative from your company and interested in this offer, please fill out the form below and we will get in contact with you.

Cybersecurity While Traveling



In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When you're traveling— whether domestic or international—it is always important to practice safe online behavior and take proactive steps to secure Internet-enabled devices. The more we travel, the more we are at risk for cyberattacks. #BeCyberSmart and use these tips to connect with confidence while on the go.

SIMPLE TIPS TO OWN IT.

Before You Go

If you connect, you must protect.

Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software.

Back up your information.

Back up your contacts, financial data, photos, videos, and other mobile device data to another device or cloud service in case your device is compromised and you have to reset it to factory settings.

Be up to date.

Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.

Keep it locked.

Lock your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or misuse your information. Set your devices to lock after a short time and use strong PINs and passwords.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

During Your Trip

Stop auto connecting.

Some devices will automatically seek and connect to available wireless networks or Bluetooth devices. This instant connection opens the door for cyber criminals to remotely access your devices. Disable these features so that you actively choose when to connect to a safe network.

Stay protected while connected.

Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with “https://” when online shopping or banking.

Play hard to get with strangers.

Cyber criminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate—or if the email looks “phishy,” do not respond and

do not click on any links or attachments found in that email. When available use the “junk” or “block” option to no longer receive messages from a particular sender.

Never click and tell.

Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don’t realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren’t— at any given time.

Guard your mobile device.

To prevent theft and unauthorized access or loss of sensitive information, never leave your equipment—including any USB or external storage devices—unattended in a public place. Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.