CYBER SECURITY AND ADVANCED TECHNIQUES TO SAFEGUARD YOUR DATA

An actionable guide to protecting your sensitive information, your financial assets and your peace of mind.
In today’s hyperconnected world, news headlines are filled with stories about identity exposure, data breaches and other major threats to your personal information and financial assets. And while corporate attacks get most of the media attention, it’s important for individuals—especially those with significant assets—to be vigilant about cybersecurity; a financially successful individual’s wealth and complex lifestyle make them a more enticing target for cybercriminals.

This guide will provide best practices, resources and actionable advice to help you protect yourself or recover from a cyberattack.

This guide was developed in partnership with Rubica, innovators in the field of digital security for individuals and families. To learn more about their personalized security services, visit rubica.com.
# Table of Contents

<table>
<thead>
<tr>
<th>No.</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRO.</td>
<td>Your Lifestyle Affects Your Likelihood for Loss</td>
<td>3</td>
</tr>
<tr>
<td>NO. 1</td>
<td>Authentication Best Practices</td>
<td>6</td>
</tr>
<tr>
<td>NO. 2</td>
<td>Fighting Email Fraud</td>
<td>8</td>
</tr>
<tr>
<td>NO. 3</td>
<td>Protecting Your Home Network</td>
<td>10</td>
</tr>
<tr>
<td>NO. 4</td>
<td>The Internet of Things</td>
<td>13</td>
</tr>
<tr>
<td>NO. 5</td>
<td>Sharing Information with Third-Party Users</td>
<td>14</td>
</tr>
<tr>
<td>NO. 6</td>
<td>Cyber-Safe Travel</td>
<td>16</td>
</tr>
<tr>
<td>NO. 7</td>
<td>Children and the Internet</td>
<td>18</td>
</tr>
<tr>
<td>NO. 8</td>
<td>Responding to Data Breaches</td>
<td>20</td>
</tr>
<tr>
<td>NO. 9</td>
<td>If You Are Hacked</td>
<td>22</td>
</tr>
<tr>
<td>CONCL.</td>
<td>How PURE Can Help</td>
<td>24</td>
</tr>
</tbody>
</table>
Your lifestyle affects your likelihood for loss.

From phishing emails and identity theft to fraudulent money transfer requests, cybercriminals continue to find new ways to target individuals and their assets. For financially successful families, the opportunities for a cybercriminal are even more numerous, and the potential profit to be made is greater.

In these households, trusted employees or other third parties may help with tasks such as caring for children; managing finances; and maintaining homes, automobiles and valuable collections. The complexity created by this network of third parties—and the communication taking place within that system—increases exposure, no matter how trustworthy or well-intentioned the individuals. Risk also increases with the number of internet-connected devices, frequency of travel and use of the internet of things (IoT).

Common recommendations, such as following best practices when choosing passwords, enabling multifactor authentication and remaining vigilant about phishing emails, become even more important when you have more to lose. And there are more advanced precautions you can take as well.

The greater your financial assets and the larger your network, the greater the likelihood that a point of vulnerability will develop—and all it takes is one. The advice in this guide is intended to help you protect yourself, your family and your assets.

1,579
Known breaches in 2017, as of January 2018

179M
Records known to have been exposed in 2017, as of January 2018

88%
Portion of all exposed records that contained Social Security Numbers
EXPOSED THE FINANCIAL INFORMATION OF OVER 142 MILLION.
In 2017, the Equifax data breach exposed the financial information of over 142 million.
Authentication Best Practices

Everyday best practices for greater security.

The importance of good “password protocol” cannot be overstated. Passwords and login credentials are an important—and sometimes the only—layer in defending your information, particularly when you’re using services like cloud-based email or online banking. Below are recommendations to help you log in more securely.

PASSWORDS

While no password is completely undefeatable, the more complex a password is, the harder it will be to crack.

- **Strengthen your passwords.** A strong password is unique, includes upper-case and lower-case letters, numbers and special characters. Consider using a mnemonic device to help you remember complex passwords. For example, build a password from the first letter of every word in a song: TtL*hwiWYA5 (Twinkle, Twinkle Little Star with special characters and a number). We recommend placing special characters, numbers and capital letters in the middle of your password rather than only at the beginning or end.

- **Never use personal information,** such as your birth date, social security number or mother’s maiden name, as part of your password.

- **Do not reuse your passwords** across different websites and services.

- **Avoid password reset questions that anyone could answer** by simply researching you or your family through paid or public services.

- **Always protect your mobile devices with a password or passcode.** Adjust the settings on your devices so they lock if they are idle for sixty seconds or more.

MULTIFACTOR AUTHENTICATION

Also known as two-step authentication, this typically combines something you know (like your login credentials) with something you have (like your device) and something you “are” (like your fingerprint). The use of multiple data points together can greatly improve security because a hacker would need to complete multiple authentication requirements—one of which may involve a physical identifier, like a fingerprint—to access your account.

Multifactor authentication can be enabled on devices, in email and on most banking, investing and social media websites. You can read a comprehensive guide to multifactor authentication, including how to enable it on many popular websites, by visiting turnon2fa.com.

Note that the prevalence of multifactor authentication as a security measure has led to a rise in fraudulent porting of cellphone numbers. Using this technique, criminals redirect your cellphone number to their own phone in order to complete your multifactor authentication requirements. Contact your wireless carrier to inquire about the security measures they offer to help you protect your account.
Must be 8 characters or more and include a capital letter, a symbol (‘&%!#$ etc.) and a number.
Fighting Email Fraud

Avoid becoming a victim of malicious emails.

Email is one of the most common methods by which cybercriminals gather information or commit crimes. Phishing and ransomware attacks are both prevalent and potentially devastating. The information that could be exposed could enable a criminal to access bank accounts, intercept purchases and hold valuable and confidential files hostage.

1,220,523

Phishing attacks in 2016

Cybersecurity and Advanced Techniques to Safeguard Your Data | PURE Insurance
PHISHING

It’s a common situation experienced by many: you open an email from a friend containing a short message about an attractive offer that seems too good to be true. Or a trusted company tells you your account is at risk. Emails that arrive unexpectedly and prompt urgent action are often actually phishing emails, messages designed to make you reveal personal information, such as passwords and credit card numbers. There were 1,220,523 phishing attacks in 2016, a 65% increase over 2015.ii By some estimates, phishing and social engineering constitute 90% of all cyberattacks.iii

Fortunately, most phishing attacks can be easily identified and resisted through the use of reasonable caution and a healthy dose of skepticism. Above are some warning signs and best practices to follow.

Be wary of communications that make an unrealistically attractive offer or ask for personal information. Phishing emails often have a sense of urgency in the language. If the sender seems to be pushing too hard, question the validity of the message.

Legitimate companies should never ask for personal information through email. If you receive a link via email to log in to your account, don’t click on it. Instead, use your browser search bar to find the official site for the company and log in from there.

Look for misspellings, grammar or logos that aren’t quite right.

Hover over hyperlinks within the message, but don’t click. Does the web address match what you’re expecting?

Check the sender’s email address: is every single character accurate, or could this be a spoofed email very similar to an address you would recognize?

Unsolicited email warrants extra caution. If you weren’t expecting it, check it carefully.

RANSOMWARE

Some fraudulent emails contain attachments or links that enable the cybercriminal to install ransomware—malicious software enabling them to hold your files or system “hostage” until you pay a sum in ransom. In May 2017, a famous, wide-spread malware attack known as “WannaCry” affected approximately 200,000 computers throughout 150 countries.iv

The advice outlined above for phishing will also help protect you from ransomware attacks. Scrutinize any email sent with an attachment, especially if the message was unsolicited or urges you to take immediate action. Never open an attachment from someone you do not know.
Protecting Your Home Network

Reinforcing your home’s fifth wall of security.

“The default username and password of commonly available routers can be easily found online.”
The security measures in place for most home networks often pale in comparison to those enforced by workplaces, but as a location where you and your family spend a great deal of time, your home network must be thoroughly protected as well. To help secure your home network, consider the following advice.

**ANTIVIRUS & FIREWALLS**

All operating systems—including both PCs and Macs—are vulnerable to malware. Installing antivirus software is an important layer of protection, but it is important to note that no antivirus product will stop all malware. Even paid services like Norton or McAfee are not foolproof or necessarily better than free antivirus software.

Firewalls are another important layer of protection. They sit on the edge of your network and block incoming connections from unauthorized users and software. Some firewalls can also block outgoing traffic, such as a virus on your computer attempting to “call back” to its commander for instructions. Despite common misconceptions, firewalls do not replace antivirus software. Rather, they are complementary and should be enabled on both your router and your computer.

To go one step further in protecting your home network, more advanced security solutions, like an active network monitoring service that can respond to threats in real-time, can reinforce and back up your antivirus software.

**ROUTER & WI-FI**

- **Change any default router credentials.** The default username and password of commonly available routers can be easily found online, so a hacker could gain access to your network simply by seeing the username on your Wi-Fi signal.

- **Give your network, identified by its SSID (a string of characters), a strong password** so only users you know and trust can connect to your network.

- **Be alert for spoofed Wi-Fi networks.** Before logging on to any Wi-Fi network (public or private), make certain that it is the correct one and not an imposter whose name closely matches that of your own network.

- **Turn off Universal Plug and Play (UPnP),** a technology designed for convenience. It allows devices and applications to communicate with each other without additional configuration by bypassing security controls. It is a common way for attackers to exploit your network.

- **Most Wi-Fi routers allow you to create a “guest” network for your home in addition to your highly secured “main” network.** “Guest” networks can be secured with a separate password, allowing you to connect noncritical devices of third-party users. Ask your internet service provider to help you create a “guest” network on a separate subnetwork (VLAN) in order to truly segment the two. Never share your “main” network’s credentials with anyone other than members of your household.

**THE CLOUD**

While common cloud-based services (e.g., Dropbox, Google Drive and Box) are convenient and user-friendly, they also present serious security exposures. Avoid uploading personal, financial and other sensitive information to cloud-based services. Although these services might encrypt your files in transit, they are not always encrypted at rest, and the service provider has complete access to them. You should always enable multifactor authentication on any cloud-based file-sharing services to secure your login access.
BILLIONS OF CONNECTED MACHINES.
The Internet of Things

Cybercrime and the connected household.

The rapidly expanding internet of things (IoT) now encompasses billions of connected machines like smart home technology, wearables and connected cars. By some forecasts, nearly 24 billion of these devices will be connected to the internet by 2020—more than double the number of laptops, smartphones and other traditional computing devices.\(^7\)

This growth has fueled a corresponding expansion of vulnerabilities. Extra caution is needed to avoid exposing your sensitive personal information to cybercriminals. Consider the following measures:

- **Change the default credentials of your connected devices.** The default security settings are often publicly available and far from secure. You should also disable any “nonessential” services.

- **Make sure all IoT devices are running on a “guest” network that is on a separate subnetwork (VLAN) from the highly secured “main” network you use to access any online accounts that contain sensitive information.**

- **Turn off Universal Plug and Play (UPnP),** a technology designed for convenience. It allows devices and applications to communicate with each other without additional configuration by bypassing security controls. It is a common way for attackers to exploit your network.

- **Keep your device up to date.** Many IoT devices do not update themselves automatically, and many updates address security flaws.

- **Pay close attention to the data security and privacy policies of IoT manufacturers.** Many IoT devices depend on cloud services or Bluetooth connections to function fully. This makes it possible for sensitive data to sync to these services without your knowledge.

- **Know what data is collected as the devices are working and how that data can be used for nefarious purposes.** For example, data streams from smart robotic vacuums can give attackers a detailed layout of your home. Settings on a smart thermostat can give insight into your schedule, and an internet camera can be used to view their feed in real-time.

- **Screen out devices known to be insecure.** Lists of known faulty IoT devices with flaws or hard-coded accounts can be found online. Visit pureins.co/IoTissues to view an example of one of the many lists available.
Sharing Information with Third-Party Users

Addressing the human element of cybersecurity.

When it comes to protecting your assets and financial information, you must consider the potential exposure created by two-way communication. The security protocol used and followed by your asset managers, assistants, attorneys and others you’ve authorized to help manage your assets is just as important as the security of the technical systems they use.

The term social engineering refers to the use of human manipulation to convince someone to give up confidential information. For example, a cybercriminal could impersonate you via email or telephone and request that your assistant perform a money transfer. If the cybercriminal is successful, that trusted personal assistant may be tricked into depositing funds into the thief’s account.

The more information available to a cybercriminal as a result of corporate data breaches or other information leaks, the more sophisticated social engineering scams can become. The data exposed by the 2017 Equifax breach, which affected over 142 million Americans, is just one example of information that could easily help a cybercriminal conduct such a scam. Following are a few tips to help you prevent information shared with third parties from falling into the wrong hands.

### MONEY TRANSFERS

Make sure you have established protocols for dealing with money transfers and other sensitive communications:

- **Require oral confirmation** and the use of a code word or phrase before processing money transfers.
- **Implement additional protections with your phone provider,** like a verbal code word or multifactor authentication, to prevent someone from forwarding or stealing your phone number in order to intercept the call-back from your bank.
- **Set up a different, hard-to-identify email address** used solely for your financial accounts.
- **Encrypt USB devices**, hard drives and other methods of transporting or transmitting personally identifiable information.
- **Ask your financial institution about their policy regarding stolen funds.** All institutions have their own policies in place for this; if you are not satisfied with their response, consider another institution.
- **Request additional layers of security** (such as multifactor authentication) be satisfied before any transactions can take place.
REAL ESTATE AND OTHER HIGH-VALUE TRANSACTIONS

Buying or selling real estate, whether it is your primary residence or an investment property, presents a unique set of fraud and cybersecurity risks. These are high-value transactions, and in most cases, a substantial amount of information about the transaction is publicly available. Cybercriminals can monitor online listing sites to learn when a transaction is likely to occur and identify the listing agent. That can lead them to the identity of other key parties who will be involved in the transaction, such as legal and escrow teams. They can then impersonate these individuals (usually through phishing campaigns) in an attempt to trick you into sending them money.

In addition, when you buy a home, you will likely engage with the seller’s legal and/or escrow firms. However, you may not be familiar with these firms or the individuals who work for them. Common cybersecurity precautions, such as conducting a “call back” to confirm the details of a wire transfer, could be difficult to verify since all relationships are new.

- If you receive an email regarding the transaction, especially if that email instructs you to transfer funds, be on the lookout for red flags that the sender is not who they say they are. Check their email address, not just their display name, to be sure that every character is correct. (For example, is the email from joe@sellersbank.com or joe@sellerssbank.com?) Also check the signature line, images and language in the email for anything that seems out of place.

- Before any funds change hands, always pick up the phone to double-check the information associated with the transaction. Be relentless in asking for verification of all account details.

- Always call to get verbal confirmation regarding any changes to the deal. When you receive a request for payment, do not call the number provided within the request itself; instead, call the main office of the company you know you are dealing with. Speak with two separate people associated with the deal with whom you have spoken before.
Cyber-Safe Travel

Remaining safe from cybercrime while on the road.

While cybercrime can occur anywhere and at any time, special precautions are required during travel. You must protect your data and devices while you are away from the secure networks you rely upon at home. You should also avoid broadcasting that you are away and your home is empty. Here are some best practices to make a central part of your travel plans.

**SECURE DEVICES AND CONNECTIONS**

- If you’ll be traveling in regions known for cyber espionage activities, consider leaving your primary personal devices at home. Take a separate phone and laptop, and have your phone calls and emails forwarded to them. That way, if your device or communications are compromised, the potential exposure is limited to the data on those devices rather than all the sensitive data on your primary device. If you must bring your primary devices, leave them in airplane mode and use a separate phone for communications.

- Public Wi-Fi at hotels, airports and cafes is notoriously unsecure. Avoid using these networks by obtaining a Mi-Fi (personal mobile Wi-Fi device) from your cellular carrier. Mi-Fis create a personal mobile internet connection with a unique password, and almost all Mi-Fis use WPA2, the preferred form of wireless encryption. You can also achieve a similar result by using a virtual private network (VPN) service, which can be downloaded to your device as an app. Providers such as Rubica can also encrypt your device traffic through a VPN and add even more layers of security.

- If one of your devices is ever lost or stolen, you will want to remove all sensitive data as soon as possible in order to mitigate unauthorized access. You can enable remote wipe capabilities for phones via services like Find My iPhone and Lookout Mobile.

**EMAIL AND SOCIAL MEDIA BEST PRACTICES**

- Post carefully and retroactively. Don’t advertise on social media about being away from home by live-posting photos and updates. Knowing you are away from home, and potentially unavailable to verify financial transactions, gives criminals the chance to exploit both your cyber and physical vulnerabilities.

- Set up a separate email account for long stays abroad: consider opening a throw-away email account for periods of extended travel. Have your regular emails forwarded to this account during the travel period to limit information exposure, in the event this email is compromised during travel.

- Use a generic “out of office” message. Don’t telegraph that you are away from home by revealing the details of your trip. Keep it simple. For example, “My response to your email may be delayed. Please contact ____ for any urgent needs.”

**MAKING INTERNATIONAL PURCHASES**

- Inform your bank that you will be traveling out of the country. Ask them to monitor your account for large or uncommon expenses.

- Carry and use a single, designated credit card for all international transactions. Ask your credit card company to monitor transactions on this card more closely.

- Monitor your bank and credit card statements closely upon your return in order to spot fraudulent transactions more quickly.
ADVICE TO GIVE YOUR CHILDREN

■ Some people you meet online may not be who they say they are, so it's best to avoid communicating with anyone you don’t know. Tell a parent or trusted adult if a stranger tries to communicate with you, and don’t accept friend requests from people you don’t know.

■ Use a nickname rather than your real name.

■ Set your profile to private so only your friends can see it.

■ Avoid sharing personal information such as your full name, address, mobile number, school and photos. If such information is required for something important, ask a parent first.

■ Be cautious about the links you click to avoid installing malware. Cybercriminals use many tactics to coerce people, especially children, into clicking on malicious links, including fake apps, plug-ins and enticing offers. These malicious links may show up in social media feeds or blogs and chatrooms.

■ Don’t accept offers that sound too good to be true. They most likely are, and you or your parents could end up with an unexpected bill—or worse. When in doubt, ask a parent.

■ Avoid accessing public Wi-Fi networks; even those that require a password are not secure.

■ Never give out your password.

■ Don’t commit or tolerate cyberbullying. Tell a parent if you see it.

■ Be careful when playing online games. Keep all chats relevant to the game, use a private chatroom and only with people you know. Never spend real money in a game without asking a parent first.

ADDITIONAL STEPS FOR PARENTS

■ Install parental control software. Both Windows and Mac offer free options that are excellent.

■ Set up unique profiles. If your children use a shared device, set up separate user accounts for them with limited permissions and higher security settings.

■ Ensure their antivirus software is up to date.

■ Review your kids’ social media profiles. It never hurts to check in to ensure they are not at risk.

Even highly responsible children can increase a household’s cyber-risk. They are more trusting than adults, and so they may inadvertently engage with cybercriminals in gaming or social media situations. They may also be aware of new techniques to circumvent parental controls.
THEY ARE MORE TRUSTING
Responding to Data Breaches

Protecting yourself in the wake of major data breaches.

Do not underestimate the severity of the breaches that have made recent headlines. Between credit rating agencies, banks and web service providers, it is reasonable to assume that your confidential information may have been compromised. In addition to bank accounts and credit card numbers, your social security number, birthday, addresses and even driver’s license information may be available to cybercriminals. This creates the serious potential for a broad range of fraudulent activity, including:

- Accessing your existing lines of credit and bank accounts
- Opening credit cards, bank accounts or lines of credit in your name
- Filing a fraudulent tax return in your name before you file for yourself
- Launching phishing attacks, fraudulent emails that appear to come from legitimate sources and try to convince you to provide sensitive information
Under normal circumstances, you should request and review your credit reports on a regular basis and consider signing up for a credit monitoring service. After a major breach, it is also advisable to place a freeze on your reports with all four credit bureaus. Here is what you need to know about this course of action:

- Freezing your credit report restricts access to your report by anyone—including you—who is attempting to open a line of credit or take another action that requires a credit pull.
- In some states, freezing your reports is free, but in others, there is typically a small cost associated with the action.
- Freezing your reports does not affect your credit score or prevent you from obtaining your free annual credit report that is guaranteed to you by law.
- If you want to apply for a credit card, mortgage, new job, etc., you’ll have to manually lift the freeze. Costs and lead times vary, so check with the credit reporting agencies in advance.
- After you request the freeze, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. You will need this information if you choose to lift the freeze.

**FREEZING YOUR CREDIT SCORE**

You can freeze your credit by contacting each reporting agency:

<table>
<thead>
<tr>
<th>Agency</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equifax</td>
<td>1.800.349.9960</td>
</tr>
<tr>
<td>Experian</td>
<td>1.888.397.3742</td>
</tr>
<tr>
<td>TransUnion</td>
<td>1.888.909.8872</td>
</tr>
<tr>
<td>Innovis</td>
<td>1.800.540.2505</td>
</tr>
</tbody>
</table>
If You Are Hacked

How to respond when an account is compromised.

A recent study by the Pew Research Center found that 64% of Americans reported that they had experienced a major data breach, including 35% who had an account number or other sensitive information compromised. Sensible precautions to secure your online information can help you avoid joining this statistic, but given the increasing severity and frequency of cyberattacks, there is no perfect solution. If you are hacked, the advice below can help minimize your exposure and better secure your accounts going forward.

IMMEDIATE ACTIONS

- Change your password as soon as you are aware your account has been hacked. Do this from a device that you know is not compromised or infected with malware.
- Log out of the compromised account(s) on all devices.
- Check the login logs for your account(s). Most cloud services track each and every time you log in to an account. This allows you to see when and from where that account has been accessed.
- If a financial account has been hacked, immediately inform the financial institution and add a fraud alert to your credit report. This will make it harder to open a new account under your name if your identity has been stolen. Adding a fraud alert is free, good for 90 days, and if you add it to one credit-reporting agency, it will be reported to the other three.
IMMEDIATE ACTIONS (CONT.)

- It may be prudent to cancel accounts that have been compromised and replace them with a new credit card, investment and/or bank account.
- If your email address was compromised when the account was hacked, consider establishing a new email address that you only use for banking, investment, health care and other accounts that hold sensitive information.
- If your phone number was compromised, consider getting a new cell phone number, particularly if you have services that use multifactor authentication or a verbal call-back for verification.

REDUCING THE LIKELIHOOD OF A FUTURE ATTACK

- Strengthen your password with more special characters, upper- and lower-case letters and numbers. Avoid using real words or personal information in your passwords.
- Enable multiactor authentication on all your accounts and devices.
- If available, enable account login notifications.
- Set up credit card alerts to notify you when a transaction occurs so that you can identify fraudulent charges quickly.
- When considering monitoring services, it is important to note the difference between identity-theft monitoring and cybersecurity monitoring. Both can be beneficial, but cybersecurity monitoring is intended to help prevent cybercrime, while identity-theft monitoring is intended to help you react more quickly if fraudulent activity has already occurred.
PURE Starling® Fraud and Cyber Fraud Coverage*

PURE Starling is an optional endorsement designed to enhance our High Value Homeowners policy by adding coverage for losses caused by fraud and cybercrime as well as access to resources to help you recover if you become a victim.

It includes broad coverage with limits of either $100,000, $250,000 or $1 million; services to help you assess, prevent and respond to fraud and cyber threats; and claims-handling by cybersecurity experts. It includes:

Online and Offline Fraud Coverage. Our coverage was designed to reimburse you for financial loss due to fraud, whether it’s committed online or in the physical world. Coverage also applies if your authorized account user—such as a personal assistant or family office manager—is the target of a fraudulent scheme that exposes your finances.

Cyber Extortion Coverage. In the event of an online attack targeting you or a family member that results in a demand for money to prevent the damage or distribution of content, or to restore access to the functionality of your device, PURE’s coverage will provide for payment as directed by the extortion threat. It also affords immediate access to crisis management advice from a subject matter expert who can assist you with how to best respond to the threat.

Systems Attacks Coverage. Should you become the target of a cyberattack, PURE’s policy will provide coverage for the cost of a professional to reinstall damaged software, remove malicious code, reconfigure your device or system and replace electronic data that has been lost or corrupted.

Coverage Provided by PURE’s Homeowners Policy*

PURE’s High Value Homeowners Policy provides coverage for:

Liability. For claims and lawsuits brought against you as a result of cyber-related property damage or personal injury, we will pay the defense costs and damages, up to the liability limit on the policy. Examples could include your child being accused of cyberbullying, a hacker—using your social profile—posting slanderous comments or a cybercriminal exposing your personal correspondence that is damaging to a third party.

Identity Theft Restoration. Following an identity theft incident, we will pay the full cost for an identity restoration consultant to restore your credit record and personal identity.
SERVICES

PURE CyberSafe Solutions™

Cyber Advice Line. Cyber Risk specialists are available to assist you with specific questions or concerns regarding the prevention, detection and response to cyberattacks.

For assistance, call 855.573.7873 | 9AM – 8PM ET | Monday through Friday

CyberSafe Fundamentals Check. As part of our in-home PURE360™ Risk Management Consultation, PURE Risk Managers will conduct a 9-point cyber risk assessment designed to help you identify and mitigate major vulnerabilities in your home network, devices and online activities.

Custom Support and Services Provided by Rubica

PURE has identified Rubica, innovators in the field of digital personal security, as a provider of fee-based active cyber security monitoring. By installing the Rubica app on all of your devices, you will be joining Rubica’s secure and private network which is monitored 24/7 by an elite team of U.S.-based cyber experts. All Rubica customers have unlimited access to Rubica experts for all their cyber security questions.

Identity Protection Services by AllClear ID

Through our preferred identity theft protection provider, you can obtain complimentary monitoring and restoration services.

Credit Monitoring. They will monitor your credit report, alerting you when banks or creditors use your identity to open new accounts. The alerts contain detailed information, allowing you to recognize whether the activity is fraudulent.

Identity Repair. If you become the victim of identity theft, they will initiate the dispute process and help you return your identity to its pre-fraud state. This service is available for all family members.
ABOUT PURE

Privilege Underwriters Reciprocal Exchange (PURE) is a member-owned insurer for responsible families with homes insured for $1 million or more. Designed from the ground up in 2006, PURE has grown by 30% or more each year since inception by providing what is widely considered to be the best service experience in the industry—helping our membership feel smarter, safer and more resilient. We offer best-in-class, customizable coverage throughout the U.S. for high-value homes, automobiles, jewelry, art & other collections, personal liability, watercraft, flood and fraud & cyber. Inspired by some of the finest policyholder-owned companies in the world, PURE emphasizes alignment of interests and transparency. Thanks to a low cost of capital, careful member selection, and proactive risk management, PURE members report average annual savings of more than 20% on their Homeowners insurance*. Visit pureinsurance.com for more information.**

ABOUT RUBICA

Rubica is a cybersecurity company that provides consumers with a dedicated digital security team to protect themselves, their families and their assets against cyberattacks. Their application allows this team to monitor traffic to and from consumers’ devices 24/7 in order to block malicious items, detect and address suspicious activity, resolve issues for consumers behind the scenes and provide concierge support and service. Rubica’s team of experts has elite government-level experience, including with the NSA, U.S. Navy and MI-6 British Intelligence. They have advanced degrees in network security with decades of experience in reverse-engineering malware, behavioral data analytics and threat-hunting and remediation. Visit rubica.com for more information.

ENDNOTES


ii https://www.antiphishing.org/apwg-news-center

iii Rubica, Inc.


vi http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

*Average annual savings on homeowners insurance for members reporting prior carrier premiums from Jan. 2011 through Jan 2018. Actual savings, if any, may vary. **Actual coverage is subject to the policy terms and conditions as issued as well as the facts and circumstances of the individual claims presented. All products, services and discounts may not be available in all jurisdictions. The material in this document is descriptive and advisory in nature. No liability is assumed by reason of the information. It is offered as a resource to be used together with your professional advisors in maintaining a loss prevention program. PURE® refers to Privilege Underwriters Reciprocal Exchange, a Florida-domiciled reciprocal insurer and member of the PURE Group of Insurance Companies. PURE Risk Management, LLC (PRM), a for-profit entity, serves as PURE’s Attorney-In-Fact for a fee. PURE membership requires an executed Subscriber’s Agreement & Power of Attorney. Visit pureinsurance.com for details. Trademarks are property of PRM and used with permission. ©2017 PRM. All Rights Reserved. 44 South Broadway, Suite 301, White Plains, New York 10601. PURE HNW Insurance Services, CA Lic. 0179885. v 3.20.18