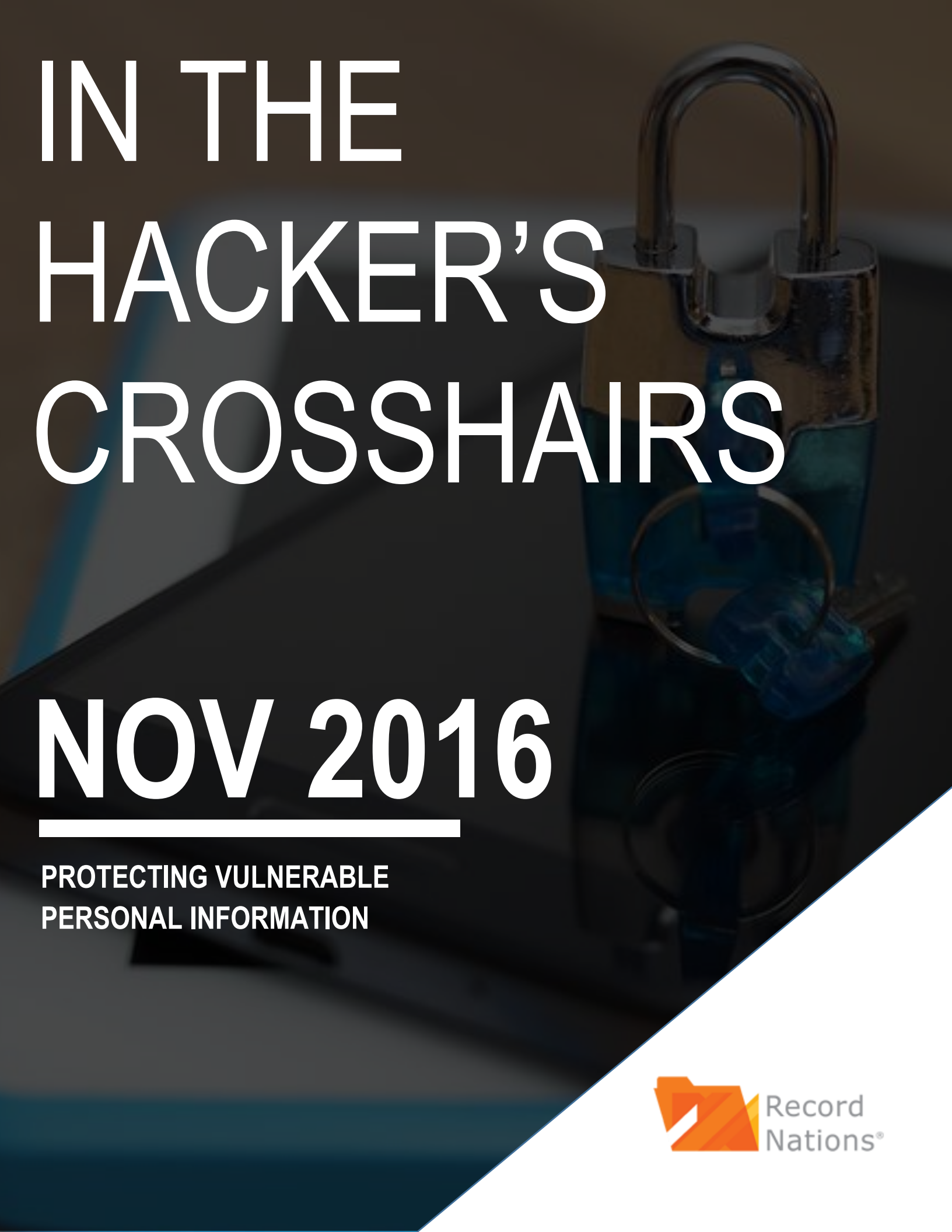

IN THE HACKER'S CROSSHAIRS

NOV 2016

PROTECTING VULNERABLE PERSONAL INFORMATION

Record Nations®

777 S WADSWORTH BLVD 3-250
LAKEWOOD, CO 80226

RECORDNATIONS.COM

LOOKING THROUGH A HACKER'S LENS

BY RYAN MCHUGH

From massive email scandals to high-profile data breaches shaking large companies to their foundations, the growing threat of data breaches and hackers stealing personal information is sending shockwaves through online communities today.

While anyone keeping up with recent news is certainly aware of the impact hackers are having, many people are now asking a more troubling question: How do I stay protected?

Before answering those questions however, the first step people need to take is actually identifying what specifically attackers are targeting and how exactly they're getting their hands on it. By understanding how others have unfortunately fallen victim to hackers, a proactive person can take the proper steps to avoid making the same mistakes.

Ranging from digital vandals infiltrating social media accounts to deface websites and delete information, to sophisticated identity thieves and malicious hacking groups penetrating networks to steal personal and proprietary information, hackers use the internet as a weapon rather than a tool.

Like any predator, hackers hunt for the easiest prey, and although the common security systems and technology has improved today, the tactics these malicious individuals use are also constantly adapting to find vulnerabilities in networks, systems, and devices—and now usually without you even realizing.

Always in search of the low hanging fruit, the primary target for hackers is where personal information is most vulnerable—online.

Although you may be the only one sitting at your computer, whenever data is sent and received over the internet that information is much like a public conversation others can overhear. From online banking and transactions to email and entertainment accounts, your personally identifiable information is all over the internet.

Throughout this in-depth white paper, we take you through the various vulnerabilities exposing personal information today, looking through the lens of hackers to provide a better idea of the information and weaknesses attackers look to exploit, as well as best practices for ensuring your personal information is securely managed and protected from hacking.

HOW HACKERS INFILTRATE PPI : IDENTIFYING GAPS IN YOUR DEFENSES

Both individuals and businesses alike use computer networks and servers to create a central location for connecting various devices like computers, printers, televisions, and other devices.

While they provide connections between multiple devices for accessing media and files, wireless networks are also typically connected to the internet as well—falling directly into the crosshairs of hackers as a result.

Many of these connected devices are chock-full of personally identifiable information (PII) such as your address, date of birth, phone number, driver's license number, and credit card numbers—and hacker tactics for getting to it are unrelenting and ever-improving, making it more essential than ever you ensure servers and networks are secure and always up-to-date.

Among the various weak spots and vulnerabilities that hackers search to exploit, here are a few of the first and most common places attackers will look for personal information:

ENTERTAINMENT AND SOCIAL MEDIA ACCOUNTS

New social media platforms and entertainment services are emerging seemingly each day—ranging from Facebook, Twitter, LinkedIn, and Instagram to Netflix, Hulu, and Youtube.

Between the growing number of accounts people now have, this also means there is an increasing number of vulnerabilities for hackers to potentially exploit and steal personally identifiable information.

Consider Facebook as just one example. Including names, birthdays, phone numbers, email addresses and even where you live, work, or travel, much of the personal

information people post and add to their accounts is made public by default.

Making this information public can often come back to bite users in the end, however, as publicly-accessible PII can not only lead to identity theft or fraud—this readily-available information is often used by hackers to provide hints for cracking weak passwords that include easy-to-remember personal information.

Furthermore, many people reuse their passwords across multiple sites and accounts, meaning that if a hacker is first able to use public PII from social media to crack one password, they can then move from one account to the next to try and see if your password is the same for other more sensitive accounts.

While sharing your Netflix account (and corresponding password) with family or friends may not seem like a big deal, imagine if your password is the same as your other accounts like email, banking, or other transaction-based websites.

Not only does this bad password reuse habit make all your accounts vulnerable instead of just one, the risk is multiplied by the number of people your password is shared with.

If they store passwords by clicking "remember me", or by saving your password anywhere in their phone, computer, or online, even your own personal security efforts would be for naught, as a hacker penetrating a friend or family members' device would be all it takes for hackers to exploit your personal information.

EMAIL

When in comes to email accounts, hackers today have taken up several different strategies for infiltrating and eventually accessing personal information.

For a more subtle approach, hackers will specifically look to target individuals sending and receiving email on unsecured networks like public WiFi. Like a public conversation, the emails you send over the unsecured networks can be intercepted—or in other words, "overheard"—by hackers who steal the PII they potentially contain.

Using malicious software otherwise known as a "sniffer", a hacker is able read sent emails as they move across a public network by accessing the numerous unsecured servers which store a variety of information during the exchange of data.
On the flip side of these difficult to detect methods data thieves and hackers are using to steal PII, however, other more direct attacks like email phishing scams also put email at risk.

Although phishing isn't exactly a new technique to look for, what makes email phishing a more prevalent concern once again, is the fact that phishing techniques are now more sophisticated, making it increasingly difficult for users to always pick out which emails are suspicious and which are from trusted sources.

Providing a perfect case in point, take for instance the flurry of email hacking that took place during the 2016 American election.

During the months leading up to election night, daily newspaper headlines were dominated by new stories of accounts and emails within Hillary Clinton's campaign team being hacked and released to the public online.

Among the numerous individuals who came into hackers' crosshairs, campaign manager John Podesta was often a primary target—and in late October of 2016, US intelligence officials may have finally uncovered the hackers' tactics.

Early in the year, an email had been sent to Podesta's account claiming to be from "The Gmail Team", and requested he change his password immediately, as someone with a Ukrainian IP address had supposedly used his password to login onto his account.

What he, or his IT staff didn't realize however, is that this email was ***not*** legitimate. While it stylistically matched Google's sites and emails, it was a traditional phishing email with a few extra features that made it difficult for even government security experts to initially realize.

Using services to shorten long, jumbled URLs and links, the hackers were able to make the link they included to change his password not actually link to the authentic Google password management page, but a scam page with a .tk domain—meaning the website was registered to the island country Tokenlau in the South Pacific.

MOBILE DEVICES

Although computing technologies have certainly developed since its beginnings in the 1980s, mobile devices have advanced at an even greater pace—swiftly moving from clunky phones with antennas, to pocket-sized smart phones providing services like internet connectivity, GPS, and other apps ranging from the helpful to playful.

Because of the speed of adoption for new mobile technologies, mobile security has been struggling to keep up with the necessary protections users need to keep their personal information out of hackers' reach.

Today developers are actively developing applications in an effort to address the issue of mobile security. While some cybersecurity companies and providers are now offering security apps through the Apple and Android app stores, some individuals however are unfortunately coming to find that when it comes to the app store, buyers should beware.

Taking up a new strategy not seen by experts before, hackers and scammers are targeting app stores, where users often will download applications without much hesitation—even sometimes allowing children access to downloading. Hoping to take advantage of this, scammers are now creating fake apps which work much like phishing emails.

Meant to look like other legitimate apps, they appear to be the apps companies provide users to access personal information and make mobile transactions, and hackers are using them more and more—especially for companies without an app already in the store.

Like other apps that provide access to location services, contact information, or saved payment information, downloading a fake app gives hackers everything they need to steal personal information.

PROTECTING YOUR PERSONAL INFORMATION: BEST PRACTICES

Given the constantly-evolving nature of hacking attacks, even the most surefire protections will eventually have small gaps for hackers to find and exploit as they expand their range of tactics.

Despite this though, there are a few strategies you can follow to prevent the threat of identity theft and ensure your personal information is as secure as possible, including:

BREAK BAD PASSWORD HABITS

From social media and entertainment accounts, to banking and transaction websites, your passwords are among your last lines of defense between hackers and your personal information.

Unfortunately however, many users still follow bad password practices like password reuse—putting not only their Facebook and other social media accounts at risk, but also more confidential personal information that if stolen would have more serious impacts.

To minimize the chances for passwords to be stolen, be sure you avoid using basic keyboard patterns like "123456" or readily-available and easy-to-guess personal information such as your initials or birthday.

Above all, be sure to always create unique passwords for each account as well as use a variety of letters, numbers, and special characters to make passwords more difficult to crack. To help store a large number of different passwords, password manager tools are also available for providing secure storage.

DON'T BE TOO QUICK TO GIVE OUT PERSONAL INFORMATION

Whether it's a link appearing in search results or an email arriving in your inbox, keep an eye out for anything suspicious, because when something doesn't seem right, it usually isn't.

With hacking and scamming strategies such as phishing emails and fake websites meant to appear as real ones to name a few, be wary for anyone asking for your personal information.

Banks, transaction-based websites, and other organizations will ***never*** ask for you to email personal information, and will instead ask you to update personally identifiable information after securely logging onto your account on their website.

Additionally, always be sure avoid public WiFi as much as possible, and if you do need to use it be especially careful about using your passwords to access personal information, as the vulnerable data exchange on public networks can expose not just information you send and receive from email, but your email password as well.

WATCH OUT FOR SUSPICIOUS APPS

Since hackers and scammers have now expanded their malicious reach into mobile app stores as well, it's important for buyers to now think twice before tapping download.

While some fake app scammers are simply creating duplicate apps for popular existing websites and companies, others are also taking a more difficult to detect strategy of making apps for the organizations that haven't already created a mobile app.

Despite a hacker's efforts to make their fake app appear as legitimate as possible, there are several things people can look out for which may be an indicator for a suspicious app.

To ensure you aren't downloading anything which could put your personal information at risk, be sure to double-check the app description page.

Avoid descriptions with broken English, few reviews, release dates in the past several days, and even details like developer names not matching other apps by a legitimate producer with other existing apps.

CONCLUSION: FINAL CONSIDERATIONS TO KEEP IN MIND

With a wide variety of malicious tools already in hackers' tool belts, both updated as well as newly-emerging tactics for stealing personal information are cropping up each day in an effort to stay one step ahead of the securities that protect the growing wealth of information stored online in accounts and document management systems today.

From traditional email phishing scams by hackers searching for personal information and passwords, to recent fake apps plaguing mobile users just in time for shopping season in 2016, there are a number of threats to look out for, but here we've provided a few last tips to help ensure your protection bases are covered:

Protect Passwords At All Costs

Passwords are the keys to unlock the vast amounts of personal information people store in their various accounts, but despite warnings, people tend to still have bad password habits. Never use the same password across multiple accounts, and try to make passwords as long and complex as possible using a variety of numbers, letters, and special characters.

Maintain a Sense of Skepticism

Digital connectivity and the online world is becoming more and more like the wild west of older days. With advancing techniques today, hackers are taking alternative and more difficult to detect strategies for carrying out digital heists like fake mobile apps and better disguised phishing emails.

ADDITIONAL RESOURCES

“Password Protected”: The Password’s Role in Modern Document Management Systems

Ranging from social media vandalism to financial cataclysm, lost, stolen, and hacked passwords can leave a variety of impacts and losses to proprietary or personal information. In this in-depth white paper, we take a closer look both at password best practices in the online world today, as well as how password security can ultimately impact the security of document management systems in the future.

Top Mistakes You're Making Online That Hackers Love

Each day it’s more than common to simply jump on the computer and casually go about your business—posting photos, making downloads, signing up for a new account. Unfortunately however, there are less-than-friendly hackers also on the watch for the common mistakes people make as they browse. Get the breakdown on the top online mistakes you’re making here.

Identifying Information Insecurities: Keeping Your Eye on the Ball

Information storage and connection technologies and the accompanying identity theft strategies for abusing this technology have drastically improved in even the past several years. As a result, many are wondering how to bolster their own protections against similar attacks, however this first requires a thorough understanding of just what identity thieves are looking for. Learn more about the high-risk information you need to secure, as well as strategies for protecting it here.