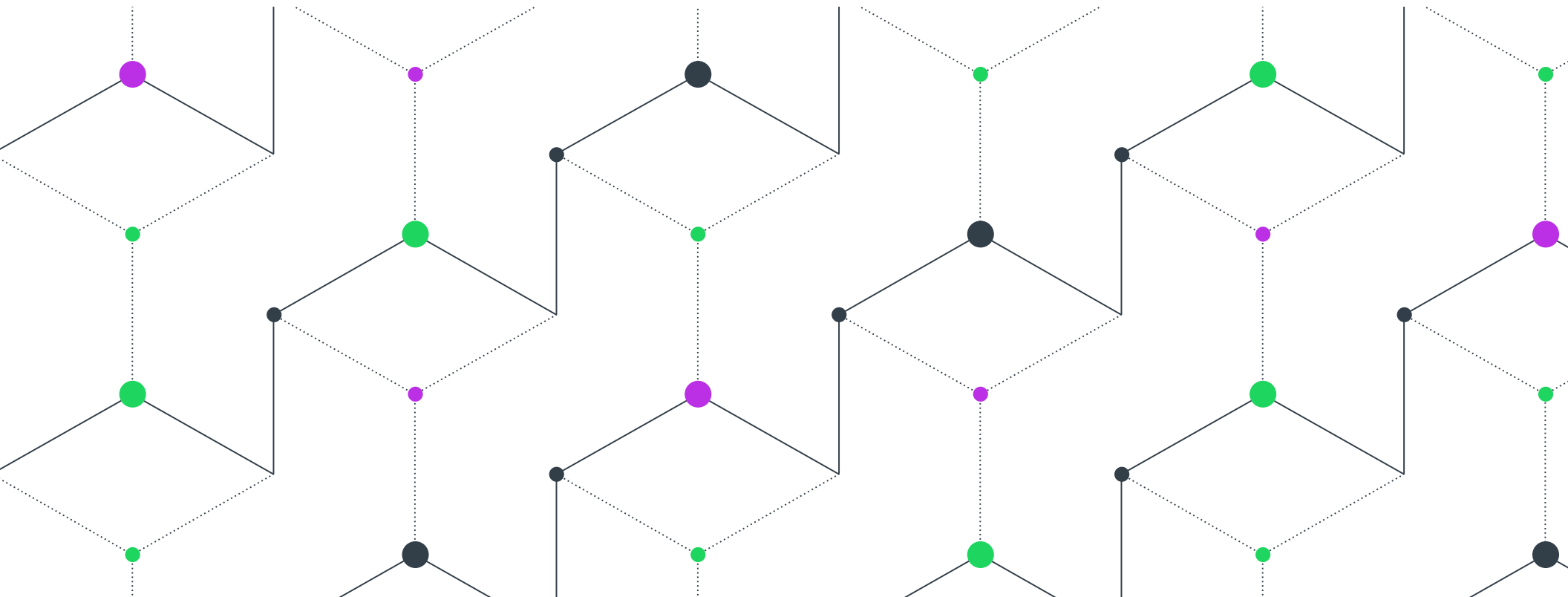revenera™

Making Software Pirates Pay

An Ecommerce Conversion Playbook

Software vendors of all sizes have been confronting the piracy problem for well over three decades.

The Business Software Alliance has estimated that the commercial value of unlicensed software is nearly $46.3 billion worldwide, but this figure only tells part of the story.

Industry leaders like Microsoft, Adobe and Autodesk have been using software intelligence to better understand who is using unlicensed versions of their software so they can develop data-driven strategies to address piracy and generate new license revenue.

Other vendors have partnered with software intelligence solutions providers to identify unpaid use of their own applications and convert those users into paying customers to the tune of more than $2.8 billion since 2010.

Whether you are a large or small software vendor, this playbook will show you:

Why you should pursue a strategy of converting unpaid users into paying customers

How you can leverage technology and software usage analytics to identify unpaid use and reach unpaid users with targeted in-application messaging that will drive conversions

Best practices for in-application messaging and ecommerce landing pages that will increase conversion rates

Why You Should Target Software Pirates

If you're like a lot of other software executives, you probably have your own impressions about what unlicensed software means. You might imagine that unpaid software is only used by students, that it only happens in China, or that people who use unlicensed software would never pay for it.

In fact, many people using unpaid software are professionals— engineers, designers and office workers from mainstream companies. They may not even know they are using pirated software, but they are using your software for legitimate business and profiting from it.

The good news is that if your application is being pirated and used, it means that people find your software valuable. It helps them achieve something that they could not do without the benefit of your application.

This is not just an optimistic way of viewing piracy: it's based on the economic realities of supply and demand. Think about it. There are thousands of pirated applications available and people and organizations are using your application to meet their needs.

The problem is that these prospective customers are leaking out of your sales funnel and you likely don't even know it and have not been able to measure the impact it has on your business. Equally alarming, your customers may also be using pirated software—limiting your opportunities to expand within existing accounts.

> TARGET

Who is Pirating Your Software?

Research from Microsoft and Adobe has identified three different types of pirate users, and their behaviors may surprise you. Let's take a closer look and learn a bit more about who these pirate users are.

"Pirate-Inclined": will never pay

The "Pirate-Inclined" think all software should be free. They're highly unlikely to pay for software, so it doesn't make sense to focus too much time on them.

"Opportunistic": want the best deal

"Opportunistic" pirates are bargain hunters. They're looking for the best deal and are willing to take some chances with less well-known online stores. According to Adobe, they are attracted to deals where the price is 70-80 percent of the list price—a "sweet spot" where the deal doesn't look too good to be true.

"Legally-Inclined": unaware of use

"Legally-Inclined" pirates have no idea that they are using pirated software. They could work at a large company where a "tech-savvy" person has installed software onto everyone's computer using only one license. They could be a home user who gets their software from a friend or relative trying to be "helpful." They might have also purchased from one of the sites that targets the Opportunistic Pirates after finding a link in a Google search.

Well-Intentioned Victims of Software Piracy

The good news is that Opportunistic and Legally-Inclined pirates are unintentionally using pirated software and are willing to pay for it. Based on research conducted by Microsoft, Adobe and Disney (and Revenera's experience converting unpaid use globally), we know that 83 percent of all pirates in mature markets are Opportunistic and Legally-Inclined and that they will pay for software.

Professionals using your software with an unpaid license will pay for software. Even organizations as established as Embraer[1], the U.S. Army[2] and the Vatican[3] have been found to be using millions of dollars in unlicensed software.

83% are well-intentioned victims of piracy and will pay for software

OPPORTUNISTIC

PIRATE-INCLINED

LEGALLY-INCLINED

Intentional Use by Businesses

Of course, some people and organizations do make a business decision to use pirated software. Perhaps the pricing is not appropriate for their market, or the licensing is so difficult to use that they deployed pirated software so users can do their jobs. They use pirated software because the repercussions seem low, or they're waiting to get caught and asked to pay.
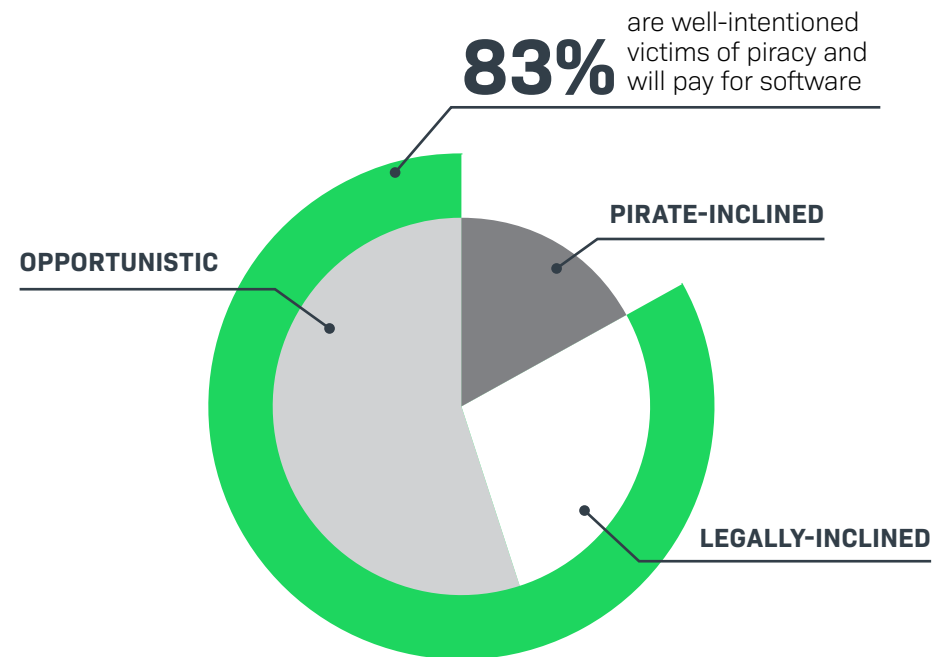
These organizations use pirated versions of your software and are competing against your paying customers by saving on software costs and undercutting your customers' prices. We've also seen cases where half of the organizations pirating software are also paying customers, installing additional copies of software illegally.

How Software Ends Up Being Used By Well Intentioned Victims of Piracy

When a vendor releases a new version of its software, piracy groups race to disable the licensing— sometimes the same day the software is released, but almost always within the first 30 days. These groups have been around for 20 to 30 years and do it to compete for bragging rights and to prove who is the best at cracking software, not to make money[5].
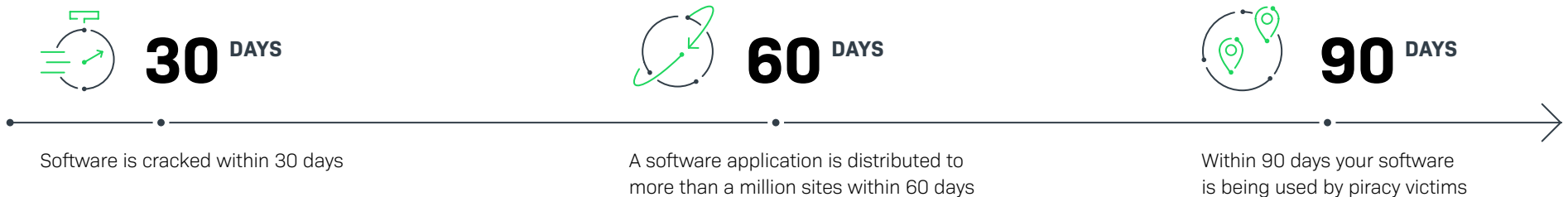
Once the piracy groups announce the release of a cracked version, a single link to your software explodes virtually across thousands of websites.

Cracked software is widely distributed and made available online through a well-established, extremely efficient, global channel of hundreds of thousands of Peer-to-Peer (P2P) sites, IRC channels, file hosting sites, industry-specific portals and forums. Once it hits this distribution channel, your software spreads around the world like wildfire.

Many of these sites don't make money by selling your software. They cater to the Pirate-Inclined and generate advertising revenue by hosting your software and driving millions of visitors to their sites.

Other sites do make money selling pirated software. As mentioned above, they target Opportunistic and Legally-Inclined pirates and sell pirated software at 70-80 percent of its list price to convey a sense of legitimacy and authenticity. Trying to stop piracy in these channels often resembles "Whac-a-Mole:" you takedown one site and two more pop up in its place.

It only takes one person in an organization to store a cracked version of your software on company servers before it rapidly spreads throughout the organization.

30 DAYS

Software is cracked within 30 days

60 DAYS

A software application is distributed to more than a million sites within 60 days

90 DAYS

Within 90 days your software is being used by piracy victims

> **IDENTIFY**

Identifying the Use of Pirated Software

Traditionally, software vendors have identified unpaid use anecdotally, through profiling, or by implementing their audit rights:

- Sales reps often suspect that an account isn't ordering more licenses because they are overusing what they've paid for.

- Support reps receive requests for help from people who don't exist in the customer database or who are using an overused or illegitimate license or activation key.

- Many vendors offer a whistleblower hotline or web form where piracy or overuse can be reported.

- License compliance teams develop profiles of likely overuse based on past experience and use them to prioritize their audit targets.

While all of these methods may ultimately uncover some unpaid use, they are not always programmatic or scalable and do not provide a real-time pulse on the unpaid use of your products.

IDENTIFY

On the other hand, adding software intelligence capabilities to your applications provides a steady stream of data and insight into who is using your applications and how they are using it. Vendors with piracy detection capabilities can use this intelligence to drive programs to convert well-intentioned victims of piracy into paying customers. Once they have identified these pirate victims, they can target them for conversion campaigns.

Vendors of B2B software share this intelligence with their compliance or inside sales teams who initiate outreach activities with these corporate pirates. This approach is less cost effective for vendors of B2C software who typically sell lower cost software to a higher volume of individual or workgroup customers. These vendors are reaching, educating and converting their unintentional victims of piracy through the use of in-application messaging. Some software vendors have built their own version of in-application messaging while others have integrated proven solutions like Revenera Compliance Intelligence with in-application messaging.

Software Intelligence Considerations

Whether you are building or buying a software intelligence solution, make sure you have these key capabilities:

1. Collect usage data
2. Transparent to end user
3. Detect misuse or tampering
4. Data aggregation, filtering and scalability
5. Correlate usage data and identify organizations
6. Identify geographic location of usage
7. Compliance with EU privacy and data storage regulations
8. Data security
9. Accessibility of data
10. Minimized engineering resources to integrate into applications
11. Drive in-application responses based on usage analytics

Reach, Educate and Convert

These well-intentioned victims of piracy have leaked out of your sales funnel. They may have come to your website at some point to learn about your solutions or even downloaded a demo version, but somewhere along their buyer's journey they began using a pirated version and fell out of your sales funnel.

Fortunately, vendors that have implemented piracy detection, software intelligence and in-application messaging have the ability to directly reach and educate those well-intentioned victims.

In the next section, we will describe how you can use in-application messaging and proven ecommerce marketing techniques to generate new license revenue from the unlicensed use of your software.

Build your In-application Messaging Strategy

In-application messaging is an essential tool to convert, nurture and retain customers. Software vendors should focus on trigger points, escalation timing, and messaging content when implementing in-application messaging. In the context of converting unpaid users, consider the strategies below to maximize conversion rates. **Remember that this is an iterative process where testing and measuring are key components to success.**

Strategy	Capability	Example
Data driven communication	Collect and understand usage activity to segment users (e.g., geography) in order to develop a targeted plan that can be tested and adjusted based on conversion rates.	Aggregated usage data indicates elevated piracy rates in Eastern Europe. Develop a regional communication messaging plan with localized content for unpaid licenses for that segment of users.
Develop usage-based scenarios	Look at trends and create thresholds when messaging will be triggered for the greatest impact in showing the value of paid versions to the user.	In lieu of a reminder at every product startup, do so after the fifth time the application has been started, or when the user wants to perform a valuable function (e.g., save, print, render, calculate, etc.).
Use a customer focused tone	Use a communication style that treats the unpaid user like a trial user. Establish a friendly, non-hostile tone, don't treat pirates like criminals. Educate, don't threaten.	"Your copy of this product may not be genuine. We recommend downloading and reinstalling the latest version directly from our website. If you still see this message, your License Key may have been compromised. Please contact customer service for assistance."
Create a communication escalation plan	Track behavior and assess trends that indicate high use. Leverage these actions to reinforce paid license value.	The first message should alert the user that the software has been tampered with and present an offer to purchase a license. If conversion does not occur at this point, the second message should gently warn the user that application functionality may be limited alongside an offer to purchase.

Response Escalation:
A Closer Look

Remember that escalation is like a nurturing campaign and use it to drive to conversions through logical steps that add urgency with each step. Analyze the usage data you have collected to customize the timing of the escalation.

RESPONSE 1

Educate + Offer

if no →
Wait X days

RESPONSE 2

Warning + Offer

if no →
Wait Y days

RESPONSE 3

Limit Functions + Offer

if no →
Wait Z days

RESPONSE 4

Control App Usage + Offer
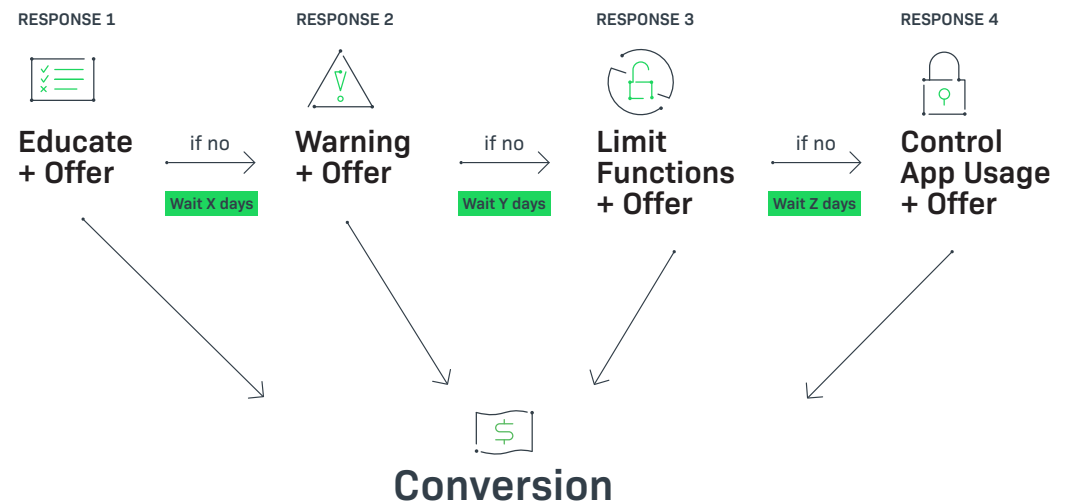
Conversion

Don't Forget:

Offering a discount can lead to higher conversion rates. Remember that many of the well-intentioned victims of piracy actually paid something for the software and believed that they were licensed users. Acknowledging this by offering a discount paves the way for a better customer relationship, too.

Best Practices for Ecommerce Landing Pages

The landing page is the unpaid user's primary entry point on the path to purchase.

To optimize for conversion, build landing pages that keep a consistent language with your website, product, and messaging. Consider that the unpaid user may already be suspicious and if they are a victim (or have a guilty conscience) they will need assurance that they are not being scammed.

Starting with these basics for landing page optimization will accelerate your learning and lead to more effective conversion of unpaid licenses.

VirusGuardian

Continue Protecting Your Computer with

VirusGuardian

There is an issue with your VirusGuardian license key. We can help get you back on track and keep your computer safe from viruses and malware.

Buy a valid license of VirusGuardian with this limited time offer:
In order to continue to protect your computer with VirusGuardian, CompuGuard must validate your software license key. For a limited time only, you can take advantage of our special offer to purchase a fully licensed version of VirusGuardian at a substantial discount.

Buy **VirusGuardian** for $99.50   **BUY NOW**
(that's 50% off our 199.00 retail price)

Learn More About the Benefits of a Genuine License of VirusGuardian Software

PRODUCT UPDATES
A/B testing is a method of comparing two versions of a webpage against each other to determine which one performs better..

VIRUS ANALYSIS
A/B testing is a method of comparing two versions of a webpage against each other to determine which one performs better..

ONLINE TRAINING
A/B testing is a method of comparing two versions of a webpage against each other to determine which one performs better..
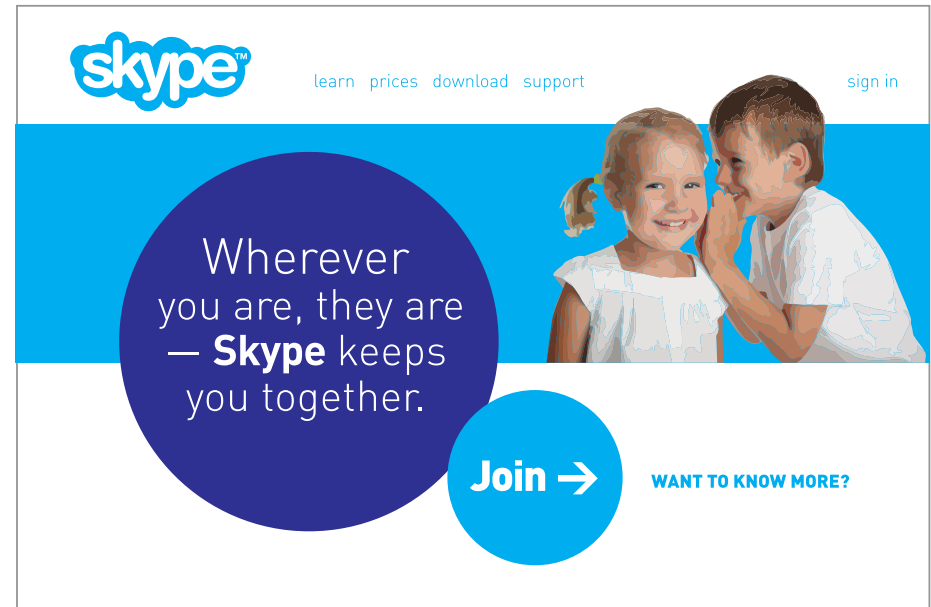
Use a Strong Call to Action (CTA)

Tip:

Use bold calls to action to direct the unpaid user to act

- Reinforce what you want the user to do using buttons like "Add to Cart", "Buy Now" and "Join"
- Use arrows and other action oriented graphics

Have a Clear Value Proposition

Tip:

Show the value of a paid license

- Highlight functionality missing in the unpaid version
- Describe the benefits of a paid license
- Explain the risks of unlicensed software

▶ BEST PRACTICES

Use Consistent Design to Establish Trust

Tip:

Use design best practices to build trust with unpaid user

- Be consistent between landing page and in-application experience
- Adhere to brand and user experience guidelines
- Test colors and layout
- Integrate with corporate marketing strategy

BEST PRACTICES

Develop Clear Content for Landing Pages

Tip:

Create effective content that speaks to the unpaid user

- Define the problem and explain the solution
- Use FAQs and Q&A to anticipate concerns and fears of unpaid users

LogoMark

Products & Services | Security Center

The Dangers of Counterfeit Software

Avoid falling victim to software pirates with these simple tips.

Software piracy is a serious matter. By using counterfeit software, you are putting your PC at risk of damage and security threats.

Counterfeit software is most often sold on bogus websites or through classified ads. Although it is possible that a counterfeit product is a good copy of the original software, it is more than likely to be defective and possibly even dangerous.

Geographical Considerations

Tip:

Adjust landing pages based on region and country, consider:

- Language and tone of content
- UI and web design
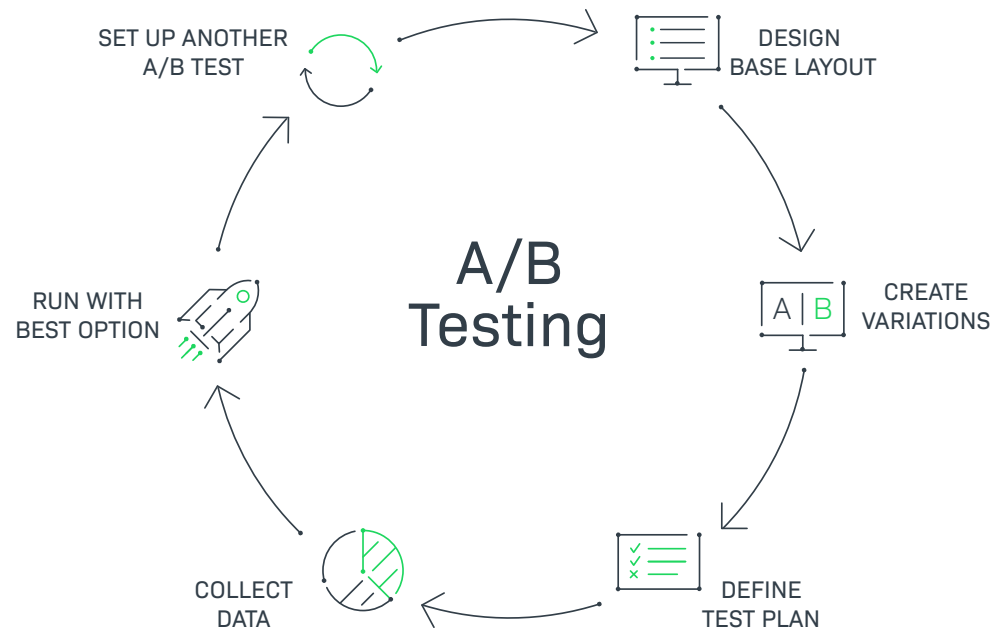- Payment methods
- Currency and pricing

A/B Testing for Unpaid Conversion

A/B testing is a method of comparing two versions of a webpage against each other to determine which one performs better. By creating an A and B version of your page you can validate new design changes, test hypotheses, and improve your website's conversion rate.

Testing takes the guesswork out of landing page optimization and enables data-backed decisions that shift business conversations from "we think" to "we know." By measuring the impact that changes have on your metrics, you can ensure that every change produces measurable and positive results.

Develop a culture of experimentation and embrace the idea of making mistakes to improve conversion with unpaid users.

SET UP ANOTHER A/B TEST

DESIGN BASE LAYOUT

A/B Testing

CREATE VARIATIONS

RUN WITH BEST OPTION

COLLECT DATA

DEFINE TEST PLAN

> NEXT STEPS

*Piracy is a **business** problem. We need to change the conversation around piracy from "company as victim" to "**customer as victim**."*

RICHARD ATKINSON
—CORPORATE DIRECTOR, GLOBAL PIRACY CONVERSION TEAM, ADOBE SYSTEMS INC.

In Conclusion

Now that you know that 83 percent of pirates will pay in mature markets and that software vendors, both large and small, are using the principles and best practices of ecommerce marketing to convert pirate users into paying customers to recover revenue, how do you pull this all together?

- Identify the application(s) that are being pirated and quantify the opportunity
- Start building your team and strategy or leverage a trusted partner

- Implement software intelligence to identify pirated use
- Develop your in-application messaging strategy to enable you to target unpaid users and escalate your responses

Revenera can help. Contact us for a free piracy assessment and to discuss appropriate strategies for converting pirated users to paying customers.

Co-author: **MIKE SCHRAMM**

—Vice President & GM eCommerce at BlueJeans by Verizon
and former General Manager Global eCommerce/Online Growth at Autodesk

FOOTNOTES.

1. http://www.atg.wa.gov/news/news-releases/washington-s-new-unfair-competition-law-protects-local-company-software-piracy

2. http://www.prnewswire.com/news-releases/us-government-pays-apptricity-50-million-233259951.html

3. http://www.alphr.com/news/security/363379/single-software-licence-shared-774-651-times

4. The Shadow Internet, Jeff Howe, WIRED: http://archive.wired.com/wired/archive/13.01/topsite.html

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**

revenera™