Security Threats to Business, the Digital Lifestyle, and the Cloud

Trend Micro Predictions for 2013 and Beyond

In 2013, managing the security of devices, small business systems, and large enterprise networks will be more complex than ever before. Users are breaking down the PC monoculture by embracing a wider variety of platforms, each with its own user interface, OS, and security model. Businesses, meanwhile, are grappling with protecting intellectual property and business information as they tackle consumerization, virtualization, and cloud platforms head-on. This divergence in computing experience will further expand opportunities for cybercriminals and other threat actors to gain profit, steal information, and sabotage their targets' operations.

Our 2013 forecasts:

1 The volume of malicious and high-risk Android apps will hit 1 million in 2013.

2 Windows 8 offers improved security—but only to consumers.

3 Cybercriminals will heavily abuse legitimate cloud services.

4 As digital technology plays a larger role in our lives, security threats will appear in unexpected places.

5 Consumers will use multiple computing platforms and devices. Securing these will be complex and difficult.

6 Politically motivated electronic-based attacks will become more destructive.

7 Cloud storage or not, data breaches will remain a threat in 2013.

8 Efforts to address global cybercrime will take two or more years to reach full implementation.

9 Conventional malware threats will only gradually evolve, with few, if any, new threats. Attacks will become more sophisticated in terms of deployment.

10 Africa will become a new safe harbor for cybercriminals.

1 The volume of malicious and high-risk Android apps will hit 1 million in 2013.

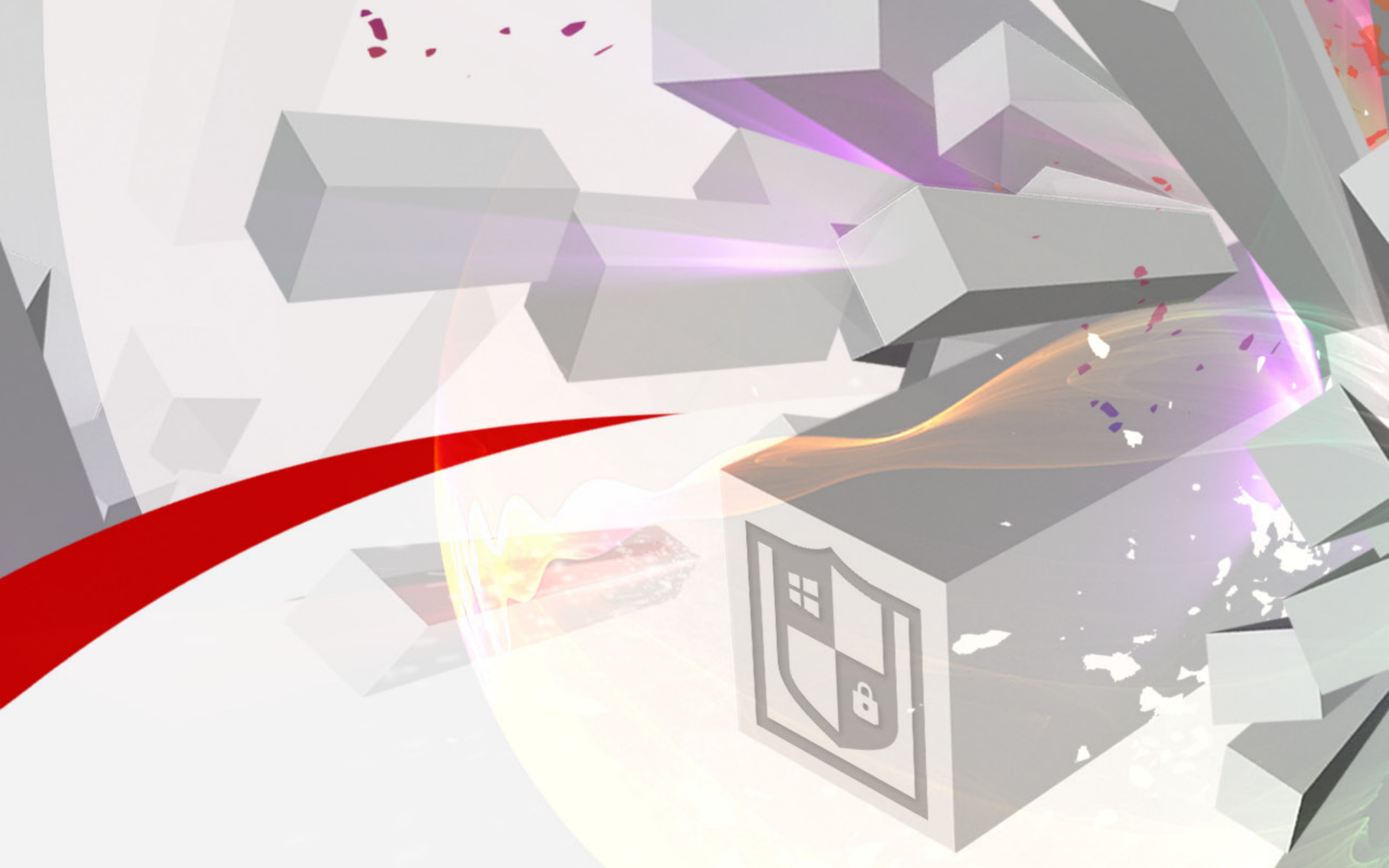
The number of malicious and high-risk Android apps, expected to reach at least 350,000 by the end of 2012, will increase threefold in 2013, broadly in line with predicted growth of the OS itself.

In terms of market share, Android may be on its way to dominating the mobile space the same way that Windows dominated the desktop/laptop arena.

Malicious and high-risk Android apps are becoming more sophisticated. An "arms race" between Android attackers and security providers is likely to occur in the coming year, much as one occurred a decade or more ago over Microsoft Windows.

Google has made improvements to the Android platform's security. App scanning in the form of Bouncer was first introduced in February and integrated into devices with the use of the latest Android version—Jelly Bean (Android 4.2)—later in the year. The improved permissions dialog box for newly installed apps made the permissions being requested more explicit.

However, these steps will not lessen the appeal of the platform to cybercriminals and thieves.



2 Windows 8 offers improved security—but only to consumers.

Windows 8 offers several key security improvements over previous versions of the OS. The most significant of these are invisible to users yet provide tangible benefits.

Secure Boot and Early Launch Anti-Malware (ELAM) do not need user input to improve security. The new OS also includes Windows® Defender, which provides a certain degree of baseline antivirus protection right out of the box.

Windows 8 includes support for Windows Store apps, which are different from traditional desktop applications. Windows Store apps are designed to act more like mobile apps, which are sandboxed by default and need Microsoft approval prior to being put up for sale or free use. This represents a more secure manner of downloading apps, very similar to how we do so for mobile OSs like Apple's iOS.

Enterprises are not likely to benefit from these improvements in 2013, as their Windows 8 adoption is expected to be limited. Gartner analysts have said they do not expect most enterprises to roll out Windows 8 in large numbers until 2014 at the earliest.[1]

[1] http://www.computerworlduk.com/news/operating-systems/3407107/windows-8-set-for-enterprise-adoption-in-2014-gartner-predicts/

3 Cybercriminals will heavily abuse legitimate cloud services.

Many businesses and individuals significantly benefitted from moving their computing needs to the cloud. Companies can reduce costs, improve ease of use, and increase reliability by moving to publicly available cloud services.

But cloud computing is equally attractive to cybercriminals. Here are examples of legitimate cloud services they have taken advantage of:

- Blogs, Facebook, and Twitter were used to transmit commands from command-and-control servers
- Google Docs, Dropbox, and Pastebin served as drop zones for exfiltrated data
- Amazon EC2 was used to act as a general-purpose malicious system

Service providers generally succeed at removing malicious users but this will not entirely stop service abuse. 2013 will definitely see more clever use of legitimate services for illegal activities.

4 As digital technology plays a larger role in our lives, security threats will appear in unexpected places.

The “digital lifestyle” increasingly links consumers’ lives to the Internet. Consumers are an attractive target and new technologies provide new venues for exploitation.

For example, imagine a high-definition TV running an existing OS like iOS, Android, or Windows. That TV may be at risk of attack because of OS vulnerabilities. The TV manufacturer may not be as capable as a computer, tablet, or smartphone vendor to fix security holes as they are discovered.

Alternately, Internet-enabled devices may use proprietary OSs and protocols designed without security as a top priority. When such devices are brought online, they can be easily compromised by enterprising attackers.

5 Consumers will use multiple computing platforms and devices. Securing these will be complex and difficult.

Yesterday's computing environment was remarkably homogenous, with Windows as the dominant platform. That will no longer be the case in 2013. Smartphones and tablets brought new OSs and apps to market with usage models that differ both from one another and from conventional desktops/laptops. Security has become a more challenging problem for users to solve—many don't even realize they are at risk!

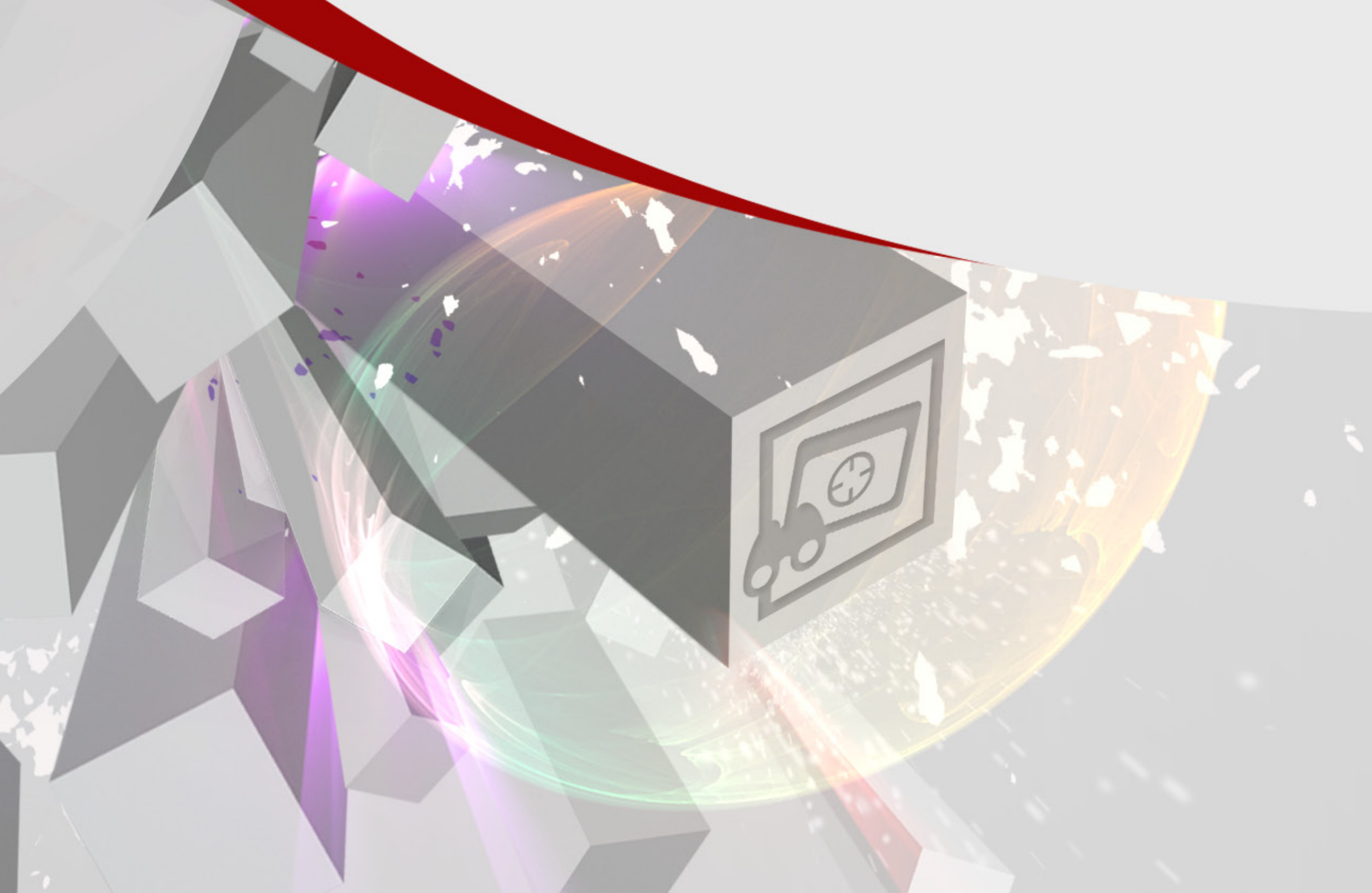
In yesterday's more uniform computing environment, it was relatively easy to educate users because fewer device types were in use. The same basic advice worked for everyone. Not in 2013. Today, each mobile platform requires a different approach to security. Similarly, as online activities move away from browsers and toward apps, it is harder to give accurate advice on security and privacy issues.

Faced with an increasing number of security options, users may just give up. They may then stick with recommended defaults, which may not be the most appropriate security and privacy settings.

6 Politically motivated electronic-based attacks will become more destructive.

In 2013, we will witness more instances of cyber attacks that modify or destroy data, or even cause physical damage to infrastructure that belong to certain countries. Such a development can be considered a logical extension of information gathering that different threat actors—be they loosely affiliated with hacker groups or state-sponsored hackers—are currently carrying out.

While it is tempting to call these attacks part of a "cyberwar," it is important to note that cyberwar involves clear acts of war—unequivocally state ordered and political in nature—performed over computer networks. Attributing these attacks to specific individuals, groups, companies, or even countries will remain a challenge.



7 Cloud storage or not, data breaches will remain a threat in 2013.

We expect data infrastructure—regardless of location—to be targeted by attacks aimed at stealing sensitive data.

As corporations move confidential information to the cloud, they will find that solutions designed to prevent large-scale information theft from on-premise servers are not as effective in a cloud-based environment. This can be due to the restrictions of the available cloud platform.

IT administrators must ensure that their cloud security solutions are properly configured and sufficient for this task.

8 Efforts to address global cybercrime will take two or more years to reach full implementation.

While some countries have established anti-cybercrime units, we expect that it will be at least 2015 before most industrialized countries are able to effectively enforce cybercrime laws.

Governments and law-enforcement agencies must develop a common understanding of cybercrime first to create a stable system that can deal with cross-border attacks.

While law-enforcement agencies are in the process of getting a foothold in dealing with cybercrime, enterprises will be left with no choice but to be more proactive in preventing attacks on their own IT infrastructure. This will be especially true for advanced persistent threat (APT) campaigns and attempting to identify who exactly is behind any attack launched.

Threat intelligence will become an important part of standard defenses for businesses that are highly at risk of being attacked.

9 Conventional malware threats will only gradually evolve, with few, if any, new threats. Attacks will become more sophisticated in terms of deployment.

Malware developers already use a wide combination of tools to achieve their goals. Developments in 2013 will only refine existing tools or respond to security vendors' efforts. A recent example is Blackhole Exploit Kit 2.0, a response to successful efforts to block spam created using Blackhole Exploit Kit 1.x.

Cybercriminals will find it more important to craft attacks to reach their intended victims without arousing suspicion than focus on specific technologies used to carry out attacks.

Cooperation between different groups in the cybercriminal underground will become more common in 2013. They will focus on specialized expertise, attacks, and targets.

10 Africa will become a new safe harbor for cybercriminals.

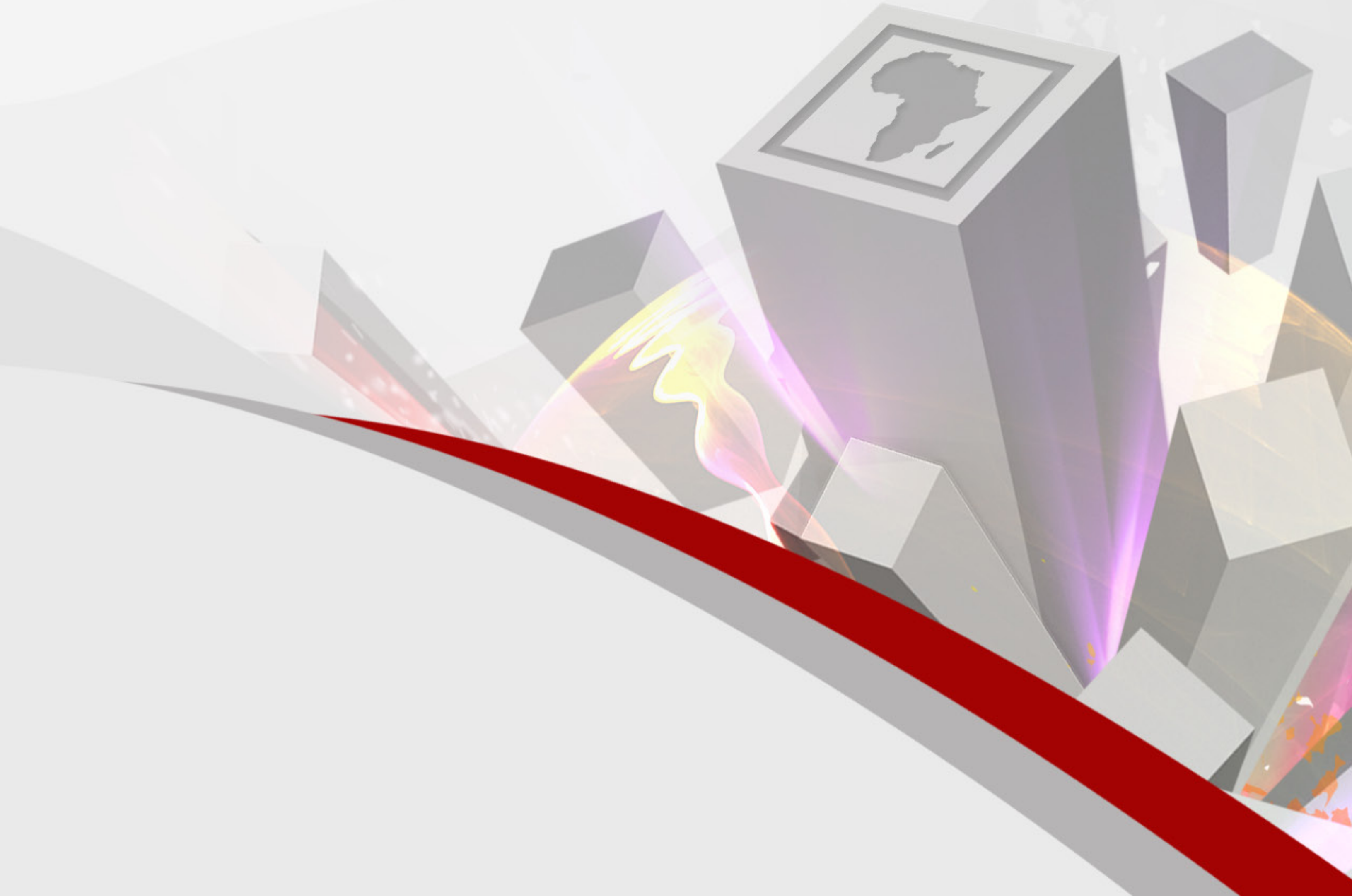
Africa, home of the legendary "419" Internet scam, is becoming home to more sophisticated cybercrime. Outsiders forced to flee more effective enforcement and prosecution in their home countries may join Africa's cybercriminals as the continent's Internet infrastructure continues to improve.

Cybercrime flourishes in regions with weak law enforcement, especially where criminals who may contribute to local economies do not target local residents and organizations.

Enforcing anti-cybercrime laws is difficult even in developed countries. If our research on the Chinese[2] and Russian[3] underground economies is any indication, cybercrime in Africa may just become a local growth industry.

[2] http://blog.trendmicro.com/trendlabs-security-intelligence/the-chinese-underground-part-1-introduction/

[3] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf



What This Means for End Users

Keep your computer current with the latest software updates and patches.

- Apply the latest security updates and patches to your software programs and OSs and enable automatic updates where possible to minimize exposure to vulnerabilities.

Protect yourself and your computer.

- If you receive an email requesting personal or confidential information, do not respond or provide the information by clicking links or calling phone numbers specified in the message. Legitimate organizations like credit card companies and banks will never request this information via email.
- Beware of unexpected or strange-looking emails and instant messages (IMs) regardless of sender. Never open attachments or click links in emails and IMs. If you trust the sender, scan the attachments before opening. Never provide personally identifiable information in your email or IM responses.
- Regularly check your bank, credit, and debit card statements to ensure that all transactions are legitimate.
- Beware of web pages requiring software installation. Scan downloaded programs before executing them.
- Do not provide personal information to unsolicited requests for information over the Web.
- If it sounds too good to be true, it probably is. If you suspect an email is spam, delete it immediately. Reject all IMs from people you do not know.
- When shopping, banking, or conducting other transactions online, make sure the website address contains an s as in https://www.bank.com.

Protect your mobile device.

- Use your smartphone's built-in security features.
- Avoid using free but unsecured Wi-Fi access.
- Scrutinize every app you download, including other users' reviews and the reputation of the developer, regardless of source.
- Understand the permissions or capabilities you are allowing an app to have on your smartphone before accepting them.
- Consider investing in a mobile security app.

Manage your passwords in a secure manner.

- Use completely random but memorable phrases as passwords instead of short, simple, and easy-to-guess ones.
- Avoid using the same password for all your login needs. For instance, do not use the same password for your bank and social network accounts.
- Change your password every few months.
- Consider using password managers.

What This Means for Businesses

Use effective solutions to protect your business.

- Deploy solutions that use cloud-based protection. The Trend Micro™ Smart Protection Network™ infrastructure rapidly and accurately identifies new threats, delivering global threat intelligence to all of our products and services. Ongoing advances in the depth and breadth of the Smart Protection Network allow us to look in more places for threat data and respond to new threats more effectively, to secure data wherever it resides.
- Develop external and local threat intelligence as part of a defense strategy against targeted attacks. Install security solutions that can provide networkwide visibility, insight, and control needed to combat APTs and targeted attacks. Consider solutions that can detect and identify evasive threats in real time and provide in-depth analysis and relevant actionable intelligence that to help assess, remediate, and defend against targeted attacks.
- As businesses move to the cloud, security becomes more crucial than ever. Data-centric protection like encryption with policy-based key management ensures the security of data in the cloud. Virtualization projects, as key steps toward fully utilizing the cloud, should consider security that is virtualization aware.
- Stay ahead of threats by reading security-related blogs and related information pages like the Threat Encyclopedia and the Security Intelligence Blog.[4]

Safeguard your customers' interests.

- Standardize company communications and let your customers know about your email and website policies. This way, you can help your customers identify legitimate messages better.

Establish and implement effective IT usage guidelines.

- Protecting your business requires educating yourself and your employees about safe computing and browsing practices. A comprehensive set of IT usage guidelines should focus on the following:
  - **Prevention:** Identify solutions, policies, and procedures to reduce risks of being attacked.
  - **Resolution:** In the event of a computer security breach, have plans and procedures in place to determine what resources to use to remedy a threat.
  - **Restitution:** Be prepared to address the repercussions of a security threat with your employees and customers to ensure that any loss of trust or business remains minimal and short-lived.

[4] http://about-threats.trendmicro.com/us/threatencyclopedia#malware and http://blog.trendmicro.com/trendlabs-security-intelligence/

TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey
to the Cloud