State of the Phish 2016

wombat security technologies

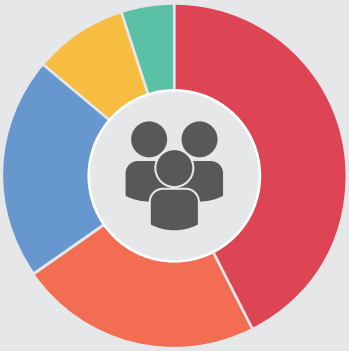
Introduction & Overview

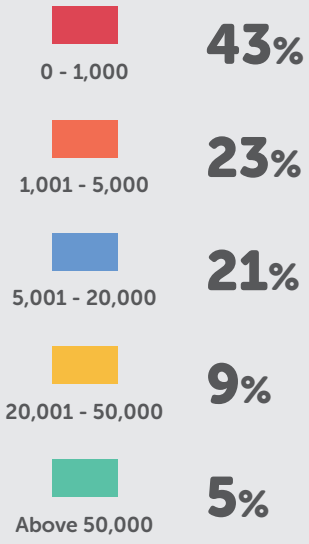
In **October 2015**, Wombat Security acquired ThreatSim®, bringing together two of the leading simulated phishing attack tools.

ThreatSim has historically prepared the State of the Phish report; this year, it was a joint effort. We compiled data from the millions of phishing attacks sent through the ThreatSim and Wombat platforms from **October 1, 2014**, through **September 30, 2015**. We also sent a survey to our database of security professionals, which includes both customers and non-customers, and received hundreds of responses. While not a scientific study, this report offers a look at those two sets of data and offers insight on running a successful anti-phishing program.

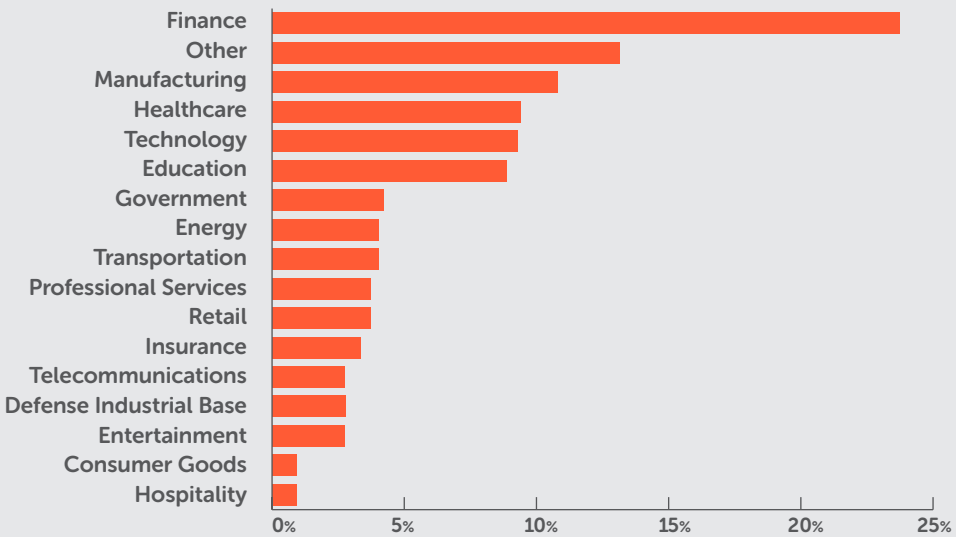
Who Participated in the Survey?

About how many employees work at your organization?





What industry does your organization belong to?



The Threat Is Still Real

As we reported last year, the threat of phishing attacks is real. News headlines and numerous studies have proven that phishing attacks are on the rise, and our survey of security professionals showed the same. Not only are more organizations reporting being the victim of phishing attacks, but the number they are experiencing has gone up. Attackers are becoming more sophisticated and varied in their approach, using multiple threat vectors.

85%
reported being the victim of a phishing attack in 2015

Up **13%** from 2014

60%
said the rate of phishing attacks has increased overall

Remember, phishing attacks are often preceded by **social engineering phone calls**, or **impostors gaining access** to information or areas they should not. You should teach your end users to not only watch out for **phishing emails**, but other **threat vectors** as well.

67%
reported experiencing spear phishing
(aka targeted attacks)

Up **22%** from 2014

55%
have experienced phishing through phone calls (vishing) and SMS Messaging (smishing)

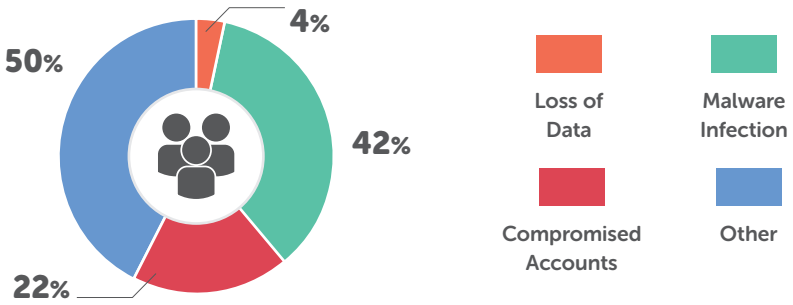
6%
have experienced phishing through USB attacks

What Is the Impact of Phishing on Your Organization?

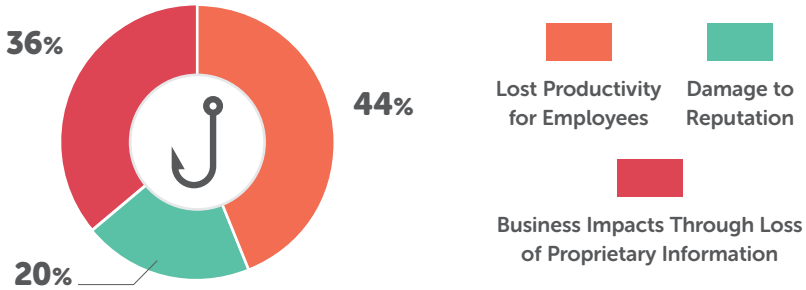
The aftermath of phishing attacks can be devastating to an organization, whether through loss of employee productivity, damage to reputation, or money lost. We surveyed security professionals to understand how they viewed the impact of phishing on their organization and how they measured the cost of phishing incidents.

What, if any, of the following impacted your organization?

(choose all that apply)



How do you measure the cost of phishing incidents?



What Is the Cost of Phishing to an Organization?

All of this begs the question: What is the cost of phishing to an organization? In late 2015, the Ponemon Institute released a paper *The Cost of Phishing and the Value of Employee Training* in which Dr. Ponemon calculated the cost of phishing for an approximately 10,000 person company. The study examined the costs of some of the very same things the security professionals we surveyed also highlighted ›

The cost to contain malware	The cost of malware not contained	Productivity losses from phishing	The cost to contain credential compromises	The cost of credential compromises not contained	**Total extrapolated cost**
$208,174	$338,098	$1,819,923	$381,920	$1,020,705	$3,768,820

As you can see, the Ponemon Institute found that the biggest amount of money lost to a phishing incident is from employee productivity losses – the very thing that most of the security professionals we surveyed identified as the way they measure the cost of phishing. The study went on to calculate the net benefit of training on phishing, and showed a return on investment specifically for Wombat's Anti-Phishing Training Suite of **50x**, proving that simulated phishing training is an effective way to reduce the impact of phishing in your organization.

What Types of Phishing Emails Are People Falling For?

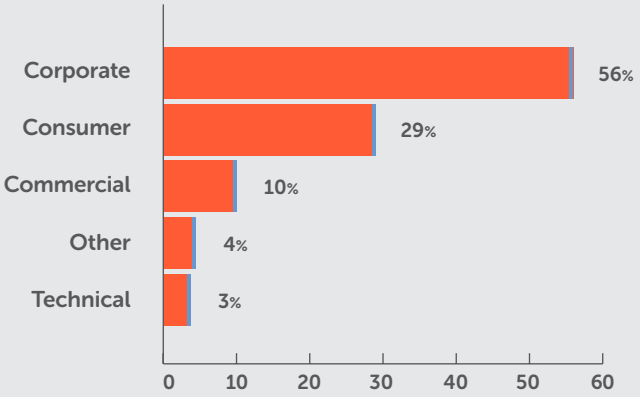
We first took a look at what was the most popular type of campaign template used by account administrators when sending simulated phishing attacks to their end users. Most administrators used corporate- and consumer-based email templates for their phishing attacks.

We then looked at the click rates associated with the different templates and found that users were most likely to click on attachments and messages they expected to see in their work inboxes, like an HR document or a shipping confirmation. They were more cautious with messages we consider to be "consumer oriented," such as gift card offers and social networking notifications.

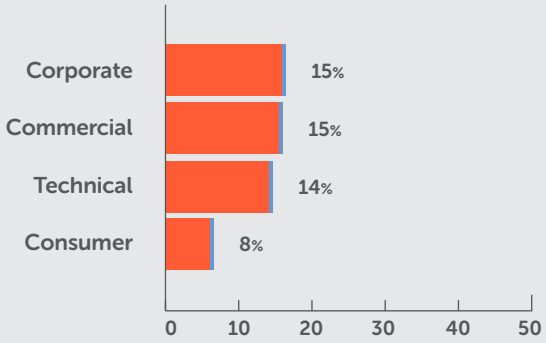
As an example, one of the most popular attacks, an Urgent Email Password Change request had a **28%** click rate.

The most popular attack template in **2015** was an electronic fax attack, which had greater than a **15%** average failure rate.

Most Used Template Types



Average Click Rate by Category



Technical Emails

These code-based emails pose as error reports or bounced emails. A "Delivery Status Notification Failure" is a popular choice in this category.

Corporate Emails

These types of emails look like official corporate communications. Examples include full mailbox notifications, spam quarantines, benefits enrollment messages, invoices, and confidential HR documents.

Commercial Emails

These are business-related emails that are not organization-specific. Sample topics include shipping confirmations, wire transfers, and insurance notifications, or auto insurance renewal.

Consumer Emails

These are the types of emails the general public gets on a daily basis that may try to replicate offers or accounts they already have. Examples include emails about frequent flier accounts, bonus miles, photo tagging, frozen accounts, big-box store memberships, social networking, gift card notifications, and more.

How Effective Is Spear Phishing?

Spear phishers often go to great lengths to gather information on key people within an organization in order to craft a personalized and convincing email. As social engineers, they aim to become someone you know and trust. Earlier on in the report, we said that **67%** reported experiencing spear phishing attacks in **2015**, and that was up **22%** from **2014**. We reviewed our data to see what the impact of personalization had on simulated phishing attack results. ›

Emails personalized with first name had click rates

19% higher

than those with no personalization

Emails personalized with last name had click rates

17% higher

than those with no personalization

However, there was good news when we looked at the effectiveness of personalization overall in mature programs. Although click rates are often high early in programs, repeated phishing simulation and training helped reduce the click rates by significant amounts as shown below. ›

	Average Click Rates in Programs Less Than 6 Months Old	Average Click Rates in Programs After 2 Years
First Name Personalization	**18%**	**7%**
Last Name Personalization	**17%**	**9%**

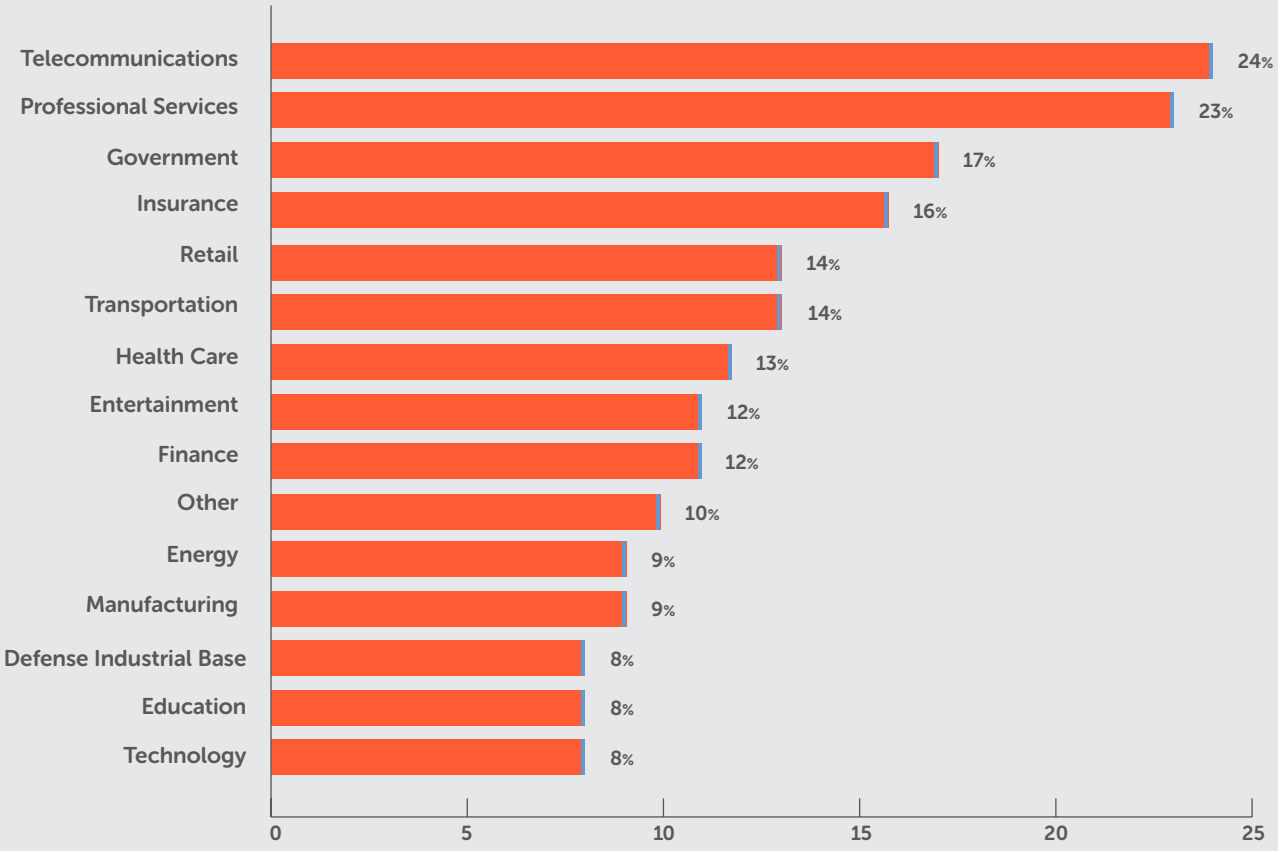
Here are some tips and questions to share with your end users to help them avoid being the victim of spear phishing attacks:

- Never give out your password via email.
- Don't log onto a website via a link sent to you in an email.
- Do you really know who is sending the email? Do you recognize the sender and their email address?
- Is the tone consistent with what you would expect from the sender?
- Is the sender asking you to open an attachment or access a website?
- Does the message contain a "call to action" or convey a sense of urgency?
- Is the domain in the URL or file name of the attachment related to the content of the message?

What Industry Clicks the Most?

For this chart, we took a look at the average click rate in each industry. While we don't have a good reason for why end users in industries like telecommunications and professional services (consulting, law and accounting firms) seem to click so much more than others, our discussions lead to multiple theories ranging from industry maturity, age of the overall workforce, to the fact that some industries may not have suffered as many breaches as others yet, which could mean that users are less aware of the risk. Whatever the reason, it is clear that security professionals in the industries at the higher end of our scale should investigate end user training to be sure their end-user population is aware of cybersecurity threats.

Average Click Rates by Industry



Which Plug-ins Are Most Vulnerable?

Many things can increase exposure to attack. One thing we can speak to with data, is plug-in vulnerability.

When end users fall for our test phish, we perform fingerprinting of the users' browsers and plug-ins. The resulting data helps to pinpoint who is at the greatest risk for a data breach.

We evaluate how likely it is that end users' plug-ins are out of date because this increases the users' exposure to attack.

Adobe PDF outdated
61% of the time

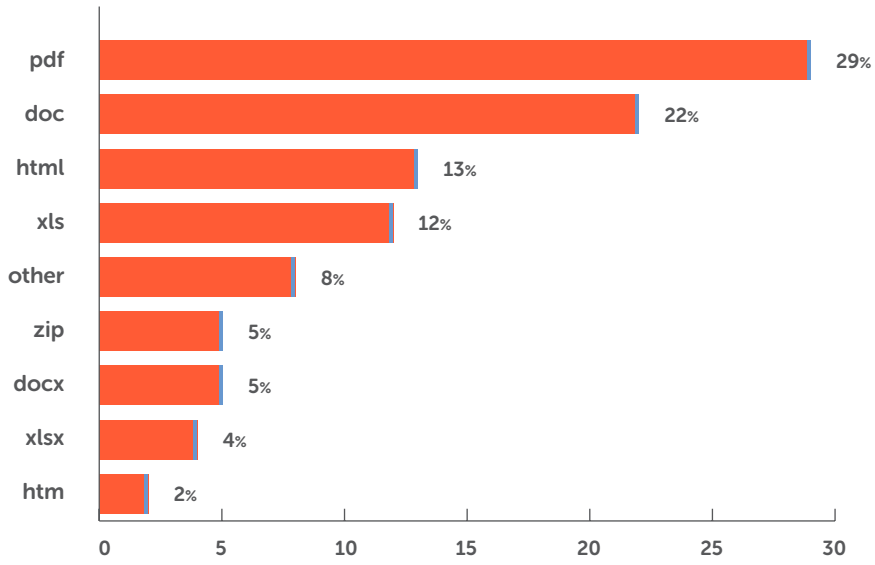
Adobe Flash outdated
46% of the time

Microsoft Silverlight outdated
27% of the time

Java outdated
25% of the time

What Do End Users Report as the Most Suspicious Attachments?

This year we looked at the types of files attached to user-reported emails, using our email reporting button, PhishAlarm®. With the rise of malware such as Dridex and Dyre, we found it encouraging to see users reporting PDF, DOC, and XLS files as suspicious. We were intrigued by some of the "outlier" file formats that were reported, including XLSM (Macro-Enabled Excel Spreadsheet). The fact that this format made it to the user where it could be reported is interesting.



How Are Organizations Protecting Themselves From Phishing Attacks?

Which of the following technologies are utilized by your organization to reduce the risk from phishing attacks?

99% Email/Spam Filters

56% Outbound Proxy Protection

50% Advanced Malware Analysis

24% URL Wrapping

Do you train end users how to identify and avoid phishing messages?

92% YES

9% NO

If yes, what of the following activities are used?

Annual security awareness training sessions (in-person, classroom style)
33%

Annual security awareness training using CBT (computer-based training)
68%

Monthly notifications or newsletters
54%

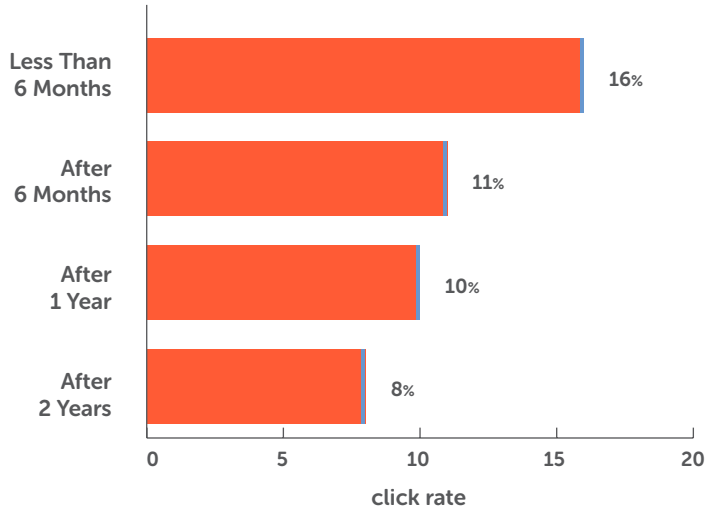
Phishing simulation exercises
70%

Other
13%

Are Simulated Phishing Attacks Effective?

Over time, simulated phishing attacks alone can be effective to reduce click rates. The data below shows that after two years, organizations can reduce click rates by **50%**. While a nice reduction, the timeline is longer for companies who only use mock phishing attacks, than it is for companies that also incorporate interactive training modules. Visit our website for case studies and proofs of concept citing much quicker reductions in click rates when using our continuous training methodology.

In 2015, the Aberdeen Group released a report, *The Last Mile in IT Security: Changing User Behavior* which stated that leading performers were **70% more likely** than lagging performers to have invested in security awareness and education for end users.



How Do You Measure?

Determining effectiveness all comes down to setting baselines and goals and measuring against them, so we were curious what security professionals were currently doing ›

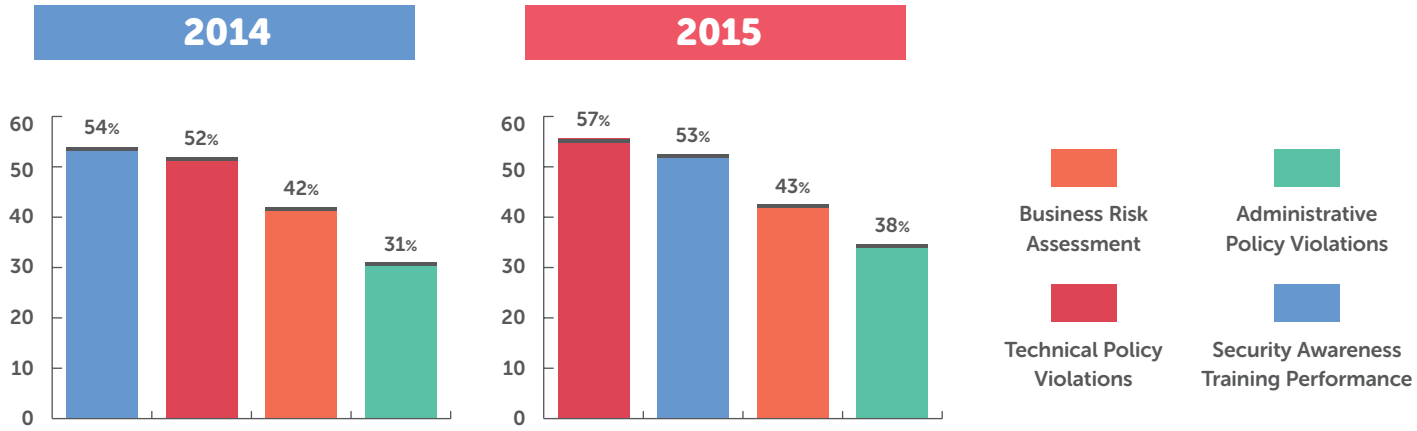
Do you measure your organization's susceptibility to phishing?

2014		2015	
61%	39%	63%	37%
YES	NO	YES	NO

Do you assess the risk each end user poses to your organization?

2014		2015	
39%	61%	44%	56%
YES	NO	YES	NO

What criteria is used to determine the risk each end user poses to your organization?



The Aberdeen Group report, *The Last Mile in IT Security: Changing User Behavior* quantifies that changing user behaviors reduces security risk by about **60%**. The report offers a Monte Carlo analysis that a Wombat Security representative can run for you to find the specific risk reduction your organization can achieve with Wombat's solutions for security awareness. You can use this data to make a business case for implementing security education at your organization.

Measurement Is the Key to Success

As you have seen through this report, mature anti-phishing programs show great results. However, if you are not measuring from the beginning, you cannot show success, be it through our programs or others. We suggest the following steps to a successful anti-phishing program. ›

Create a Plan

- Evaluate your current state of phishing attacks and set objectives for improvement.
- Communicate the program to all appropriate stakeholders.
- How will you assess vulnerability? Will you send an initial mock attack, or will you perform some other type of knowledge assessment?
- Will you assess all individuals in the business, or subsets? Decide how you want to report results.

Baseline Assessments

- Break users into functional, geographic, and access level groups as appropriate.
- Deliver a simulated phishing attack to gain a baseline vulnerability.
- Review results and compare to statistics from this report.

Communicate Your Program

- Send an initial communication outlining the steps in the program from the assessments through education.
- Explain how you will communicate training assignments, including what is a safe link in email communication so your users know what domains, web addresses and branding to look for in advance.

Simulated Attacks and Auto-Enrollment

- Deliver different simulated phishing attacks with appropriate Teachable Moments.
- Auto-enroll “clickers” in anti-phishing training modules with mandatory completion.
- “Non-clickers” can be enrolled in voluntary training that will strengthen employee knowledge about phishing.

Repeat the Cycle

A single cycle of the action plan can be executed in as little as a month or (more typically) over two months, which allows you to repeat the steps at least six times per year. As seen through results shared from our customer data, mature programs show continuously improving results over time. We strongly recommend this longevity and repetition as it drives measurable change and helps to create a culture of security awareness that extends to every level of your organization.

Want to Start Measuring Now?

No matter what you are currently doing, you can determine a baseline today. Gather report items, including current malware infections, reported and identified phishing attacks, number of IT helpdesk calls a month and any other items that you are able to measure and want to set goals for improvement. Measure monthly, or quarterly to gauge your progress.

Change Behavior. Reduce Risk.

Contact Us: wombatsecurity.com | info@wombatsecurity.com | 412.621.1484 | UK +44 (20) 3807 3472

00116SOTP