proofpoint.

CYBERSECURITY FOR THE MODERN ERA

THREE STEPS TO STOPPING MALWARE, CREDENTIAL PHISHING, EMAIL FRAUD AND MORE

www.proofpoint.com

“ONLY AMATEURS ATTACK MACHINES, PROFESSIONALS TARGET PEOPLE.”

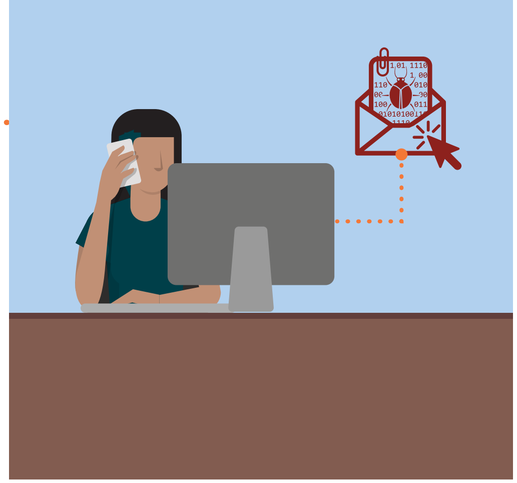
– Bruce Schneier, cryptographer, computer security and privacy specialist

The following is adapted from “Hacking Human Nature: A Practical Guide for Managing Today’s Cyber Attacks.” The book explores how cyber attacks and compliance issues are evolving and outlines how you can create a security and compliance strategy built for the way people work today.

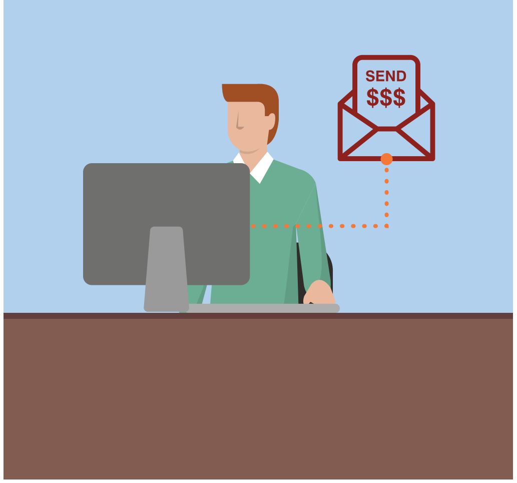
INTRODUCTION

If you're like most IT leaders, you're invested heavily in the latest security tools. Yet you're still inundated with ransomware and other advanced malware, credential phishing, email fraud and more. You're spending more time dealing with a growing volume of threats. And you're seeing a shrinking return from your security investments. That's because most of today's attacks play off human weaknesses:

1 A distracted user who clicks on a link or opens an email attachment without thinking



2 An employee who falls victim to an email believed to come from a company executive, with a seemingly reasonable request to transfer money



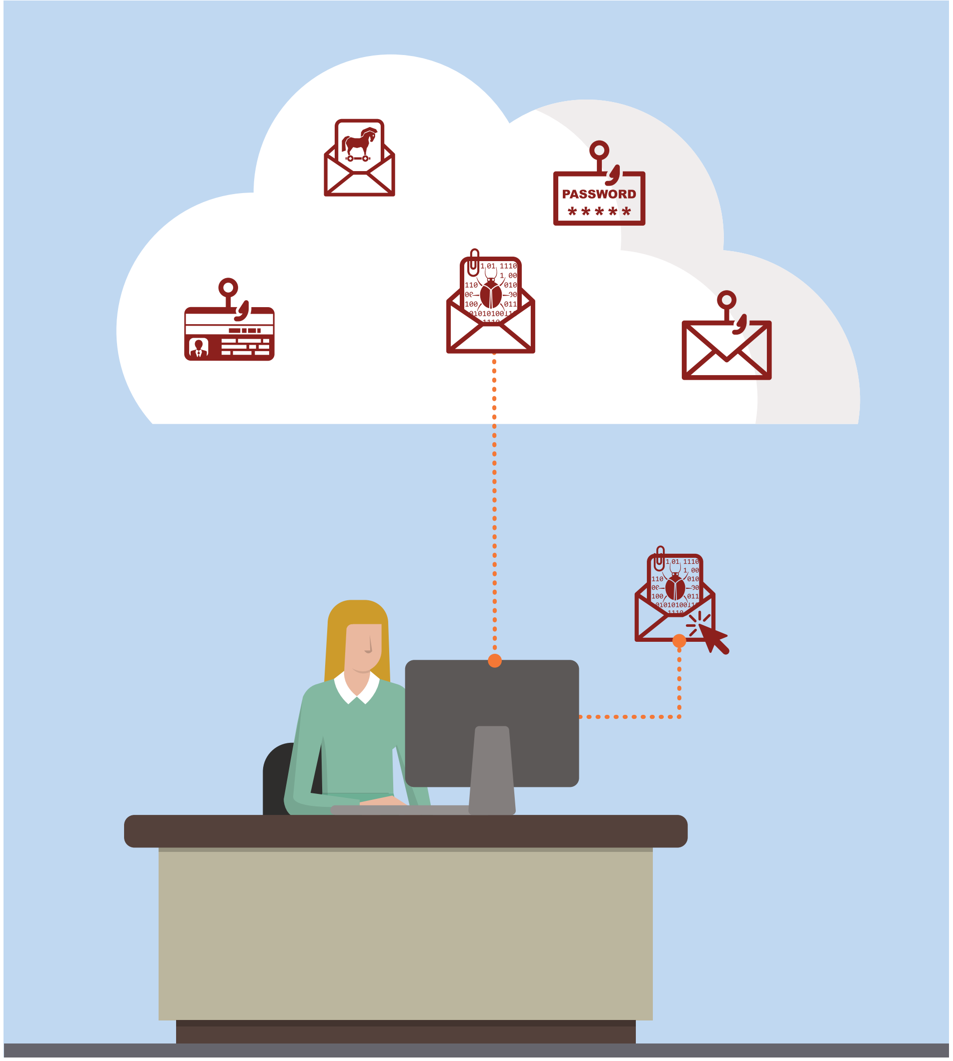
3 A customer eager to take advantage of an online discount

People, not technological weaknesses or vulnerabilities, are at the center of most attacks. Firewalls, intrusion detection and prevention systems (IDS/IPS), network defenses, endpoint antivirus software and the like are all important. But none of them address today's real security issue: people. It's time to turn the focus to humans, the principal risk factor.

Some 90% of targeted attacks start with email. These are generally phishing attacks: the email purports to come from a reputable person or company, and its apparent validity persuades the recipient to disclose personal information such as passwords or credit card numbers. Most email attacks require the victim to take some sort of action: open an attachment, allow a macro to run, click a malicious link or respond to a fraudulent request to transfer money.

Because today's attacks are aimed at people, defenses need to focus on protecting people, educating them and doing everything possible to ensure they are not tricked, exploited or compromised. How can companies put people at the heart of cybersecurity?

Here are tips on how to choose tools and solutions to improve behaviors and outcomes.



STEP 1

DEPLOY A LAYERED EMAIL DEFENSE

More than 90% of targeted attacks reach victims through email. The goal: sneak into your environment and gain access to other important assets. You need a layered defense to:

- **Detect** known, new and emerging email attacks
- **Take action** as soon as a threat is discovered
- **Address** both malware and non-malware threats
- **Protect** against spoofed and lookalike domains

MORE THAN 90%

of targeted attacks reach victims through email.

EMAIL-BORNE MALWARE

Malicious attachments and links to credential-stealing web pages get most of the media attention. But lately *ransomware* has stolen the spotlight. And its scope is expanding. No longer content to encrypt files and demand a ransom for decryption, newer variants render the entire device unusable. In any type of email malware attack, people are the trigger: they must open the email for the attack to succeed.

An effective defense should:

- Continually assess local and global IP addresses to determine whether to accept an email connection
- Recognize potentially malicious emails (such as those with links to spoofed domains)
- Block malware-carrying email before it hits the user’s inbox
- Take evasive action, such as rewriting the URL so it doesn’t point to a malicious site
- Use email authentication to block emails with spoofed sender domains

PAYLOAD-FREE THREATS

Emails without attachments or links can be just as dangerous: they can fool the recipient into disclosing sensitive information or carrying out fraudulent activities like bank transfers. Email fraud or BEC cost businesses more than $5.3 billion from October 2013 to December 2016.[1] And these threats are hard for most security products to detect. The best defense against non-malware threats is to use a tool that:

- Analyzes a wide variety of email attributes, such as sender/recipient relationship and sender reputation
- Conducts the analysis in multiple languages
- Quarantines incoming email by type

TIP

Sending a malicious message to your junk folder isn’t enough to protect you and your company. The only way to remove danger is to quarantine the suspicious message or remove it entirely via automation.

[1] FBI. “Business E-Mail Compromise: the 5 Billion Dollar Scam.” May 2017.

PERSONAL EMAIL AT WORK

Organization have no visibility into or control over cloud-based personal email services that users access from their work computer. Short of blocking personal email altogether—a solution that is not likely to be popular among employees—securing this outside channel is difficult.

SPOOFED DOMAINS

Spoofed domains, which look almost identical to legitimate domains, are often used in email or social media scams. Because the "From" address domain looks legitimate, users click on links and go to copycat sites.

An automated email fraud defense system can accurately detect who is sending email on an organization's behalf so legitimate senders can be authorized and fraudulent emails blocked. This type of system, built on top of email authentication, provides a full view of inbound and outbound email traffic.

LOOKALIKE DOMAINS

Spoofed domains are only part of the story. Criminals also register domain names that are similar to that of a known brand, for example, "rea1domain.com" instead of "realdomain.com." They commandeer your brand and goodwill to hijack advertising traffic or steal intellectual property. And they may use lookalike domains in phishing email attacks. Organizations need a detection system based on real-time threat intelligence feeds to combat this problem by:

1. **Discovering** newly registered domains on a daily basis
2. **Monitoring** threat intelligence feeds for clues to imposter sites
3. **Updating** information on bad IP addresses and URLs constantly

TECH TALK

How can you know the sender of a message is who they say they are? Implement email authentication standards like SPF, DKIM and DMARC. Learn how with this Email Authentication Kit.

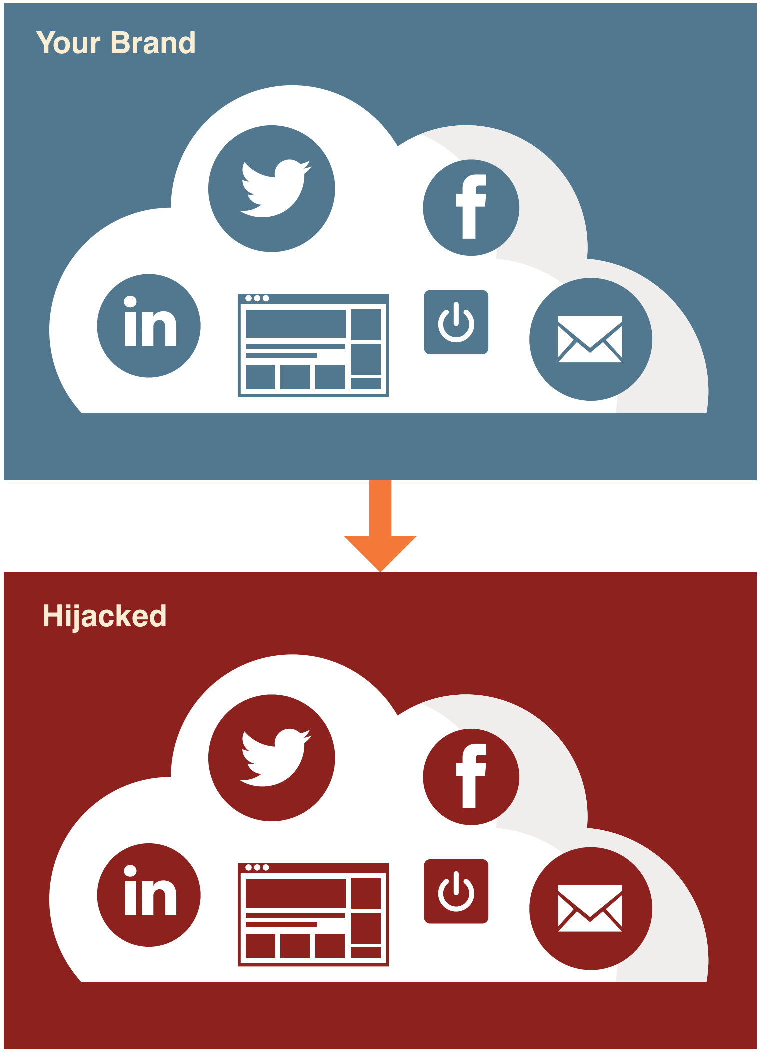
TIP

A real-time threat detection system based on threat intelligence can identify new threats and integrate minute-by-minute IP and URL information with security tools to block attackers.

STEP 2

GET VISIBILITY INTO CHANNELS YOU DON'T OWN

A strong web and social media presence is a necessity for business: companies spend billions to ensure customers can engage easily through the corporate website, Twitter, Facebook, mobile apps and other channels. Unfortunately, the same visual cues that help customers recognize your brand can be hijacked by cyber criminals. It's hard to detect or monitor bogus communication on digital channels that aren't controlled, much less protected, by your traditional security infrastructure.



LOOKALIKE DOMAINS, AGAIN

Lookalike domains and domain spoofing are not used solely for phishing campaigns. Cyber criminals may set them up for other nefarious purposes, such as to:

- Sell counterfeit goods
- Infringe on trademarks
- Post negative information or protest against the brand
- Prepare for a future attack ("parking" the domain name for later use)

A domain discovery tool can be invaluable for finding malicious domains and rendering them inoperable. Consider using a social media moderating service to automatically remove malicious or hateful content.

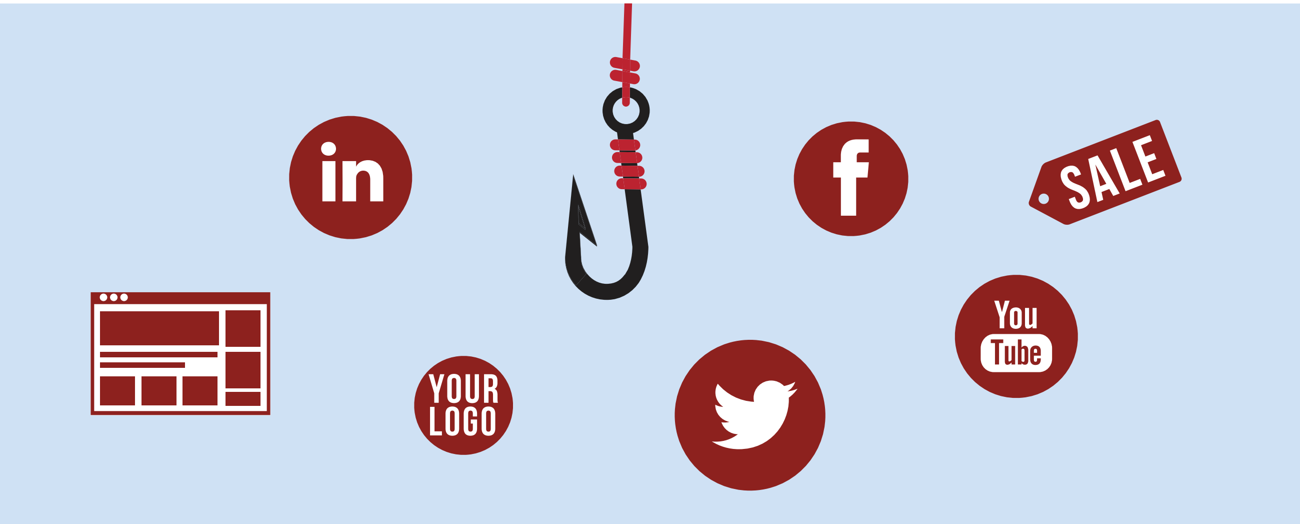
LOOKALIKE SOCIAL MEDIA ACCOUNTS

It's very easy to create a lookalike social media account that will fool all but the savviest users while defrauding customers or damaging your brand. Social media phishing is the fastest-growing social media threat, with a 150% increase from 2015 to 2016.[2] One of the most alarming new trends in fake social media accounts is angler phishing: using a fake "customer support" account that closely resembles the real corporate account to siphon off sensitive information and credentials. [See the "Digital Fraud" section in Chapter 1].

Use automated tools to monitor social networks for fraudulent accounts. Look for a tool that scans continually, alerting you when it finds an account using elements of your brand.

↑150%

Social media phishing is the fastest-growing social media threat, with a 150% increase from 2015 to 2016.



[2] Proofpoint. "Social Media Brand Fraud Report." September 2016.

APPS

Customers, employees and business partners use a multitude of mobile apps in their daily lives. Most are safe, but many are malicious. Customers trust that when they download your company app, they are getting what they expect. However, more than 16,000 developers worldwide are hard at work creating imposter apps that look like yours but steal data or send information to an unknown server.[3]

TIP

Implement a cloud app defense system that scores apps based on their relative risk and empowers you to restrict risky app behavior and quarantine or deny access to enterprise services until malicious apps are removed.

SAAS APPS: RISKY OR SAFE?

Ubiquitous SaaS apps are easily downloadable and installable without direct involvement of the IT department. Are they safe, or do they introduce risk? Even well-protected SaaS infrastructures can be compromised by apps that access corporate data with little oversight. Compliance issues can be introduced when they collect, store or retain corporate data accessed by the user—sometimes even after the person who installed it stops using it.

Fortunately, there are tools that assess the risk for apps in popular third-party markets (including unlisted and custom OAuth clients), considering:

- Permission levels
- Types of data and objects accessed by the app
- Trustworthiness of the vendor
- Trustworthiness of the app behavior

TECH TALK

Auth is an open standard that grants access without specifically sharing credentials. It has proven so vulnerable to phishing because it exploits the trust between users and well-known service providers like Google.

[3] Proofpoint. “Mobile Malware Masquerades as POS management App.” March 2017.

STEP 3

MAKE USERS RESILIENT, NOT FRUSTRATED

Some security tools create big stumbling blocks for users—and for IT as well. Look for solutions that integrate seamlessly with the normal workflow of users and IT staff alike. An intuitive UI and good performance make life easier, not harder, for users.

At the same time, avoid creating unnecessary barriers that offer few security benefits and make users less productive. That means tailoring security measures to individual users' risk. For this, you'll need insight into their unique risk factors, such as:

- How often are they targeted?
- What data and resources do they have access to?
- How meticulous they are when it comes to following security policies?

SECURITY AWARENESS TRAINING

Training users to quickly spot and report unsafe email can also help integrate security into their normal workflow.

Phishing simulations—fake email attacks launched by your own security team—are a good way to spot users most open to attack. Once you know who's more likely to bite, you can reduce their risk through:

- More training
- Tighter security controls
- Monitoring more closely for signs of account compromise

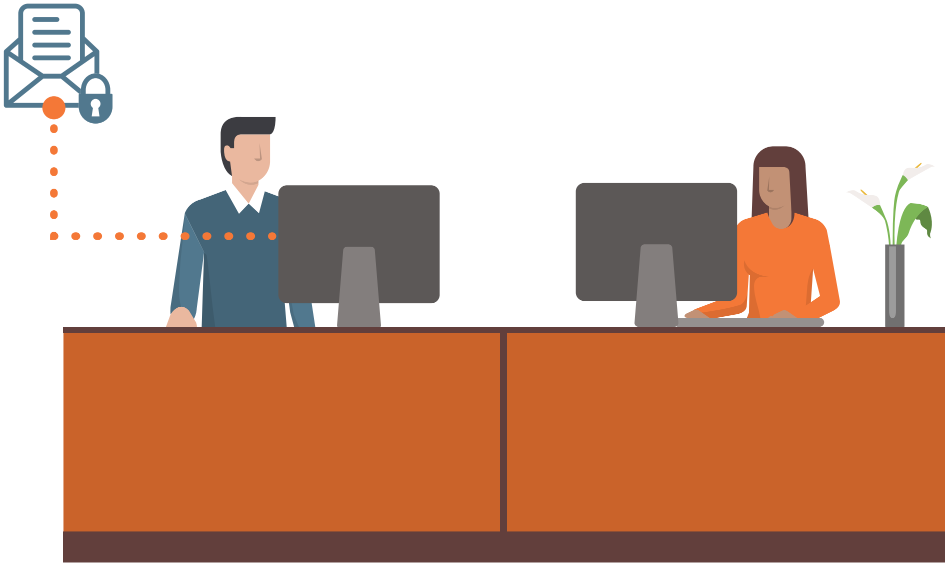
TIP

The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.

WEB AND PERSONAL EMAIL ISOLATION

Let's face it: most people use their work PC and the corporate network for some personal business. Web email and personal browsing can expose your organization to risks that are harder to control. Fortunately, you can keep your environment safe without placing stringent constraints on personal browsing.

Web isolation technology keeps personal browsing traffic, including web-based email, separate from your network. Web pages are rendered in the cloud and streamed to a secure browser on the users' PC. So if someone visits a sketchy website or opens an unsafe attachment, the threat never enters your environment.



CLOUD APP SECURITY

Businesses are flocking to cloud-based services such as Microsoft Office 365, G Suite and others. These platforms can make workplaces more flexible and reduce barriers to teamwork. But even amid this shift, people remain the biggest security risk.

That's why you need visibility into how people are using cloud apps and any third-party add-ons that connect to them. Look for a solution that can correlate user-specific risk factors with rich threat intelligence to spot and help resolve potential threats.

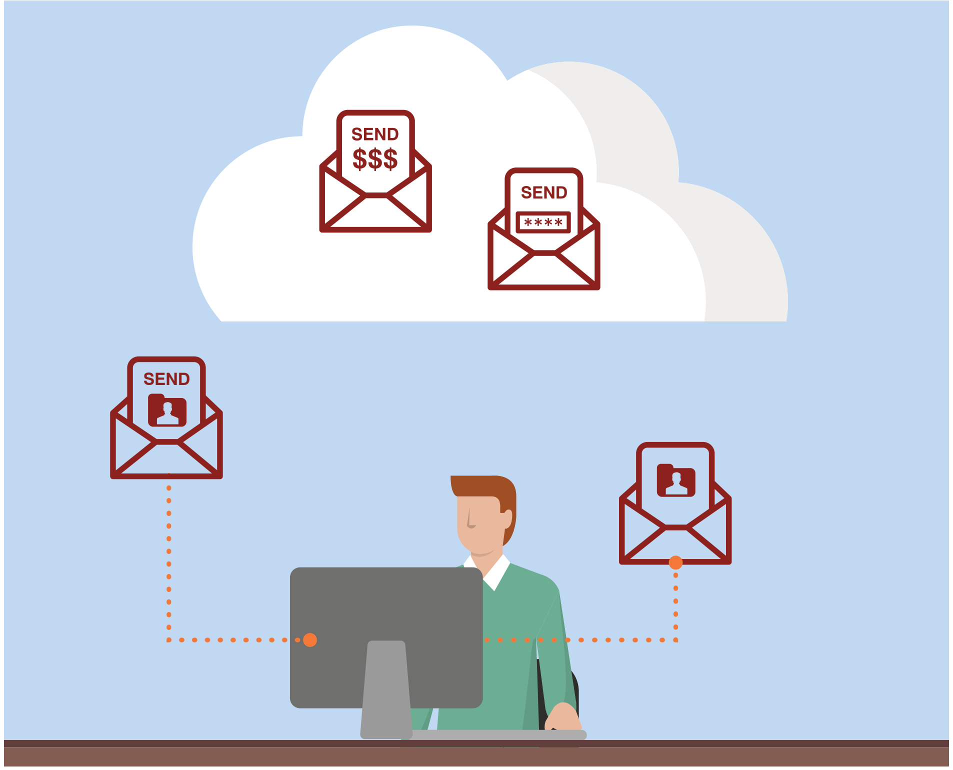
Look for cloud security solutions that can:

- Provide contextual data, such as the users' location, device, network and login time.
- Use behavioral analytics to spot unusual or suspicious activity such as excessive login attempts. These may point to brute-force attacks, where attackers try to guess the users' credentials again and again.
- Draw on global threat intelligence to check whether the IP address used in an attempted login can be trusted.
- Correlate threat activity across email and the cloud to connect the dots between credential phishing and suspicious logins.

PROTECTING CLOUD ACCOUNTS

It's no exaggeration to say that users' credentials are the key to your kingdom. When cyber criminals compromise Office 365 credentials, they can launch attacks inside and outside of your environment. They can convince users to wire money or part with sensitive data. And they can access your critical data, such as intellectual property or customer data.

Modern people-centered security means protecting these accounts from compromise.



NEXT STEPS

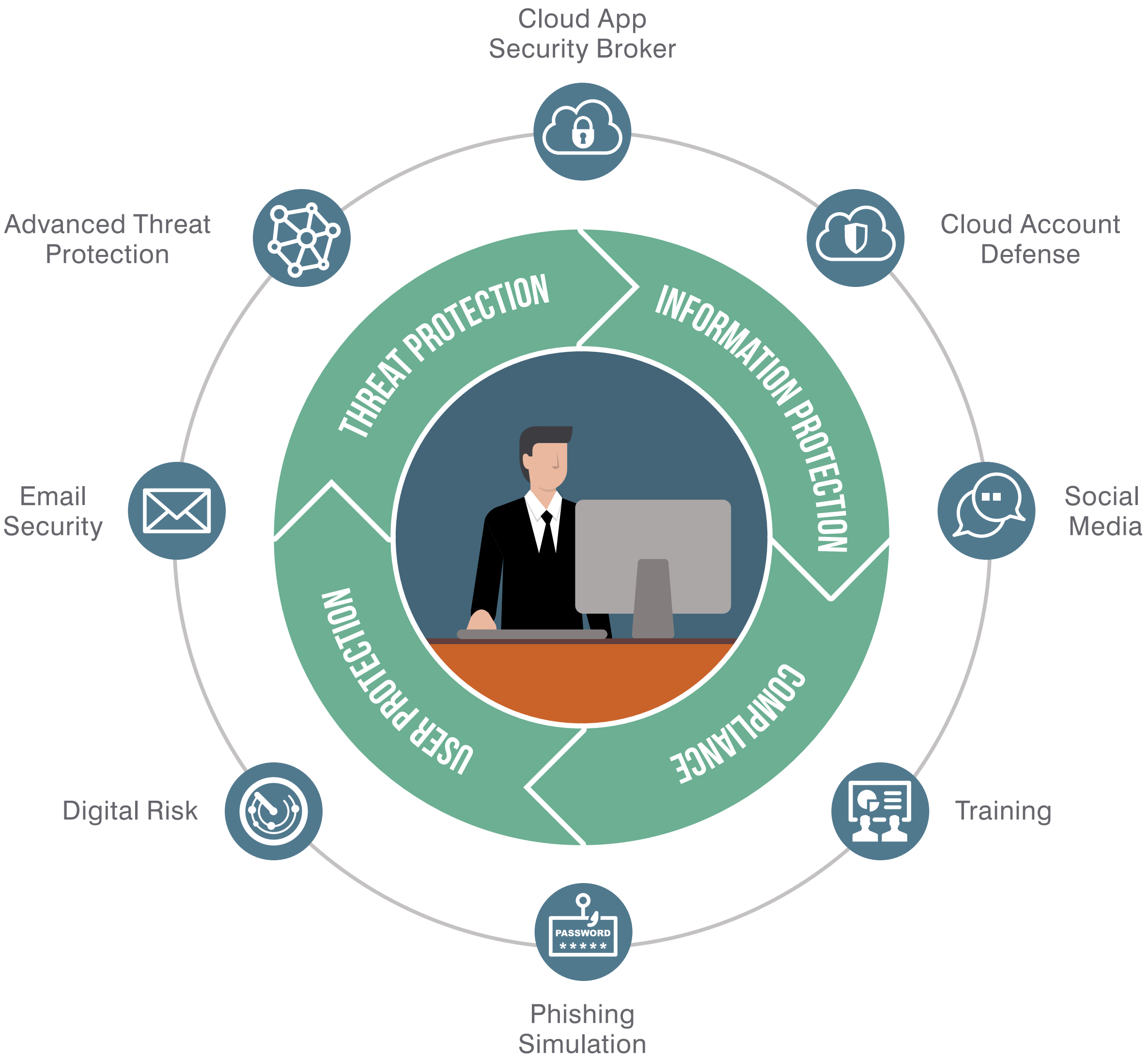
Defending against today's advanced attacks means putting people at the center of your cybersecurity and compliance strategy.

Attackers are the ultimate adapters, learning what works and what doesn't, and changing their tactics to present a moving target. But one thing is consistent: they attack people, not technology. That's why you need to shift your focus away from technical exploits and place it squarely on people.

Any organization that takes active steps to put people front and center in its security program is a step ahead of the bad guys.

Make sure your solution covers all the bases. It should be based on solid TI that matches your specific needs. And it must take human nature into account. You can't change it, so you need to work with it.

Don't just hope for the best: combat people-centered attacks with people-centered solutions.



LEARN MORE

To learn more about what a people-centered approach looks like in practice, join our webinar

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.