Fraud Education and Awareness

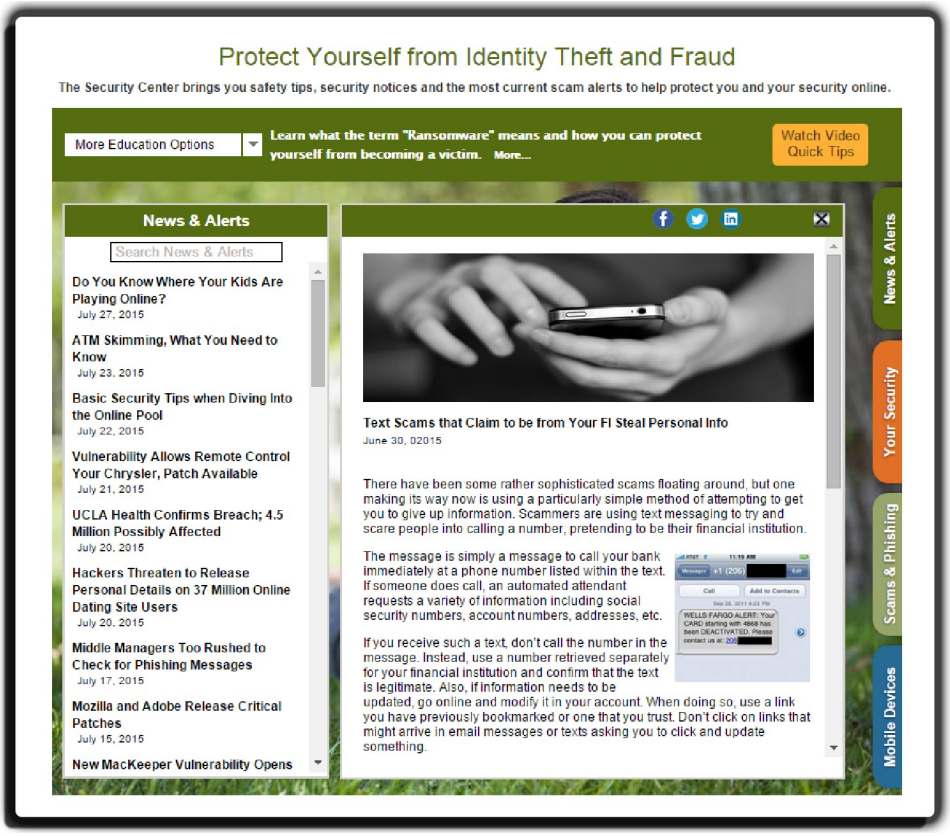
Stickley on Security

Security Education Made Easy

SoS Advisor

From scams to malware, account takeovers to credit card fraud, your customers continue to face an endless stream of potential attacks. Adding to the confusion is news outlets providing partial information that only fuels more fear. It's no wonder customers are turning to their financial institutions for real information on how they can remain secure.

SoS Advisor allows your organization to provide the information your customers need with helpful articles and tips necessary to stay one step ahead of the identity thief. It is a cost effective solution that turns your website or online banking application into a comprehensive customer security advisor.



"Response has been overwhelmingly positive. The regulators also like it as a tangible sign of commitment to staff and member security education. The Analytics help back that up."

-Ray Spreier (Chief Information Officer)
Mid Oregon Credit Union

"When customers become victims of identity theft, online banking malware or any number of other scams circulating, their organization pays the price. Keeping customers informed of the latest threats gives them a distinct advantage over the criminals."

- Jim Stickley

INCLUDED SERVICES

- Continual security updates and warnings
- Access to all SoS customer training videos
- Access to the SoS quick tips videos and player providing quick and easy security tips in under 60 seconds
- Social media support
- Customized news feeds

ADDITIONAL SERVICES

- Unique custom security videos created specifically for your organization
- Custom onsite customer training
- Remote customer training via webinar

Security Education Made Easy

Employee EDU

When over a billion dollars was stolen from financial institutions around the world, the cause was traced back to compromised employees. Target, Sony, Home Depot and even Anthem Blue Cross were also breached through mistakes made by the employees of those organizations. The reality is, no matter how secure your network, in most cases it takes just one mistake by an employee to lead to complete and total compromise.

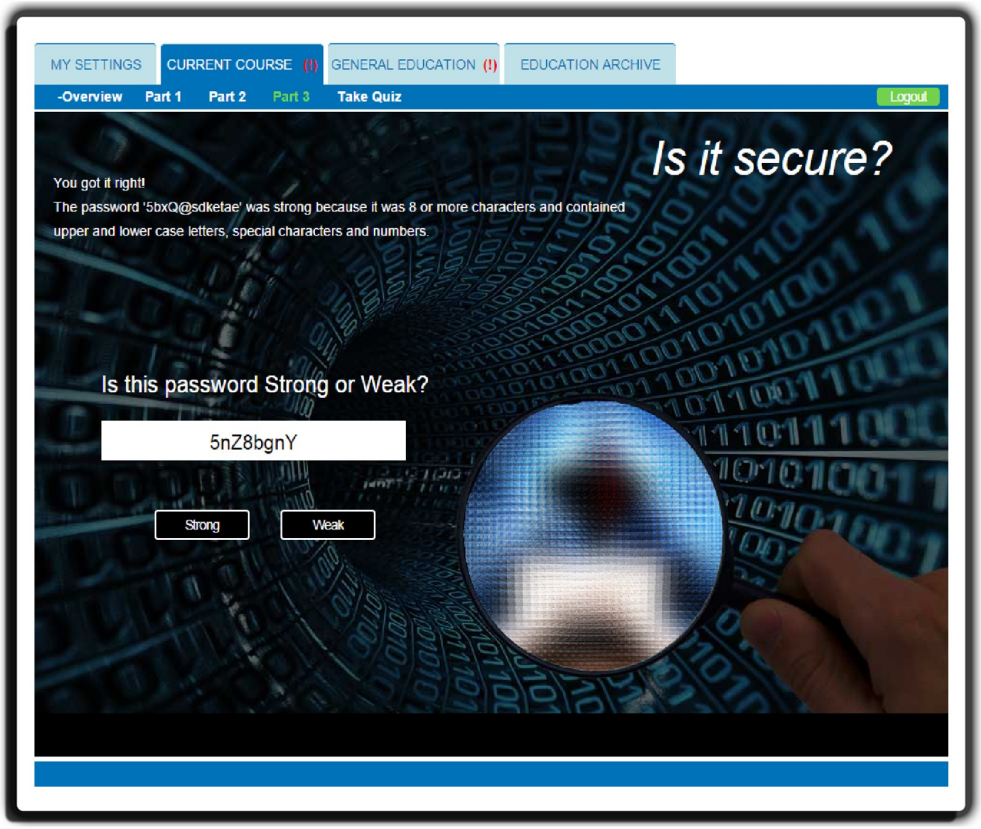
Employee EDU takes a unique approach in providing comprehensive security education and awareness training to your staff. Comprehensive quarterly education courses and continued security awareness updates ensure your staff is prepared for the latest cyber security attacks.

"One of the greatest threats to information security could actually come from within your company or organization. Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee ."

-Corporate Technology Group

"Security concerns are huge for any financial institution. Both SoS Advisor and Employee EDU keep our members and staff educated and provide the information needed to help us stay secure. "

-Leo H Lee (Director of IT)
Providence Federal Credit Union



INCLUDED SERVICES

- Quarterly security education campaigns focused on keeping your staff informed about high risk security topics
- Security awareness programs providing your employees with up-to-date security articles detailing recent security concerns and events
- Fully customizable policy and incident response training. Your organization can choose from existing courses provided by SoS that can be used immediately or modify them to fit your specific policies. In addition, you can create your own unique training courses
- "Gamification" (educational games) designed to make learning more interesting and interactive for your employees
- Detailed reporting that provides your management and regulators with the information needed to validate your continued education program
- Automated notification designed to ensure your employees are aware of new campaigns, pending courses and security advisories

Reduce Fraud Through Education and Awareness

The Next Generation Phishing Simulator & Education Solution

When employees become victims of cyber criminals, your organization pays the ultimate price. While filters, firewalls, anti-virus, and malware prevention solutions can help, the reality is that each day thousands of malicious emails are received by unsuspecting employees all over the world. In the worst cases, these employees fall victim to the included attacks.

Phishing is the most common term used to represent email attacks, but that name can often be misleading and downplay the enormous risk that comes from these types of emails. Today, criminals use phishing attacks to not only gain login credentials and confidential information, but also to gain control over desktops and ultimately the networks of the compromised systems. Through creative new emails, unpatched applications, and a never ending supply of increasingly robust malware, the phishing attack now ranks as one of the top entry points into compromised organizations throughout the world.

For over 25 years Jim Stickley has been using these techniques to compromise organizations that range from armed government facilities to community banks and credit unions. Using this unique skill set, Stickley has designed BadPhish, the world's most advanced phishing simulator and education solution. Just sending a forged email does little to test an employee. At this point, most employees are aware of basic phishing concepts and are likely to detect these types of attacks. However, as criminals become more sophisticated, so do their emails. That's why BadPhish uses a hybrid approach to phishing simulation. Now, organizations are able to choose from a vast database of predefined payloads and then use simple customizations techniques to create one of a kind tests that match the most sophisticated attacks that criminals are using today. With this design, BadPhish offers an unlimited number of unique tests that an organization can perform.

Of course testing employees is only the beginning. BadPhish also provides general security training when an employee fails a phishing test. In addition, for those organizations with Employee EDU, BadPhish has been integrated, allowing for easy customized course assignment and tracking upon failure of a phishing test. Simply put, you are no longer just simulating attacks, you are actually educating your users and validating their progress. Supporting the option to purchase one time testing or purchasing yearly service, which includes unlimited continual testing, Badphish offers a solution that fits your organizations needs and with comprehensive reporting and an easy to manage cloud-based interface, it's easy to see why BadPhish has become the next generation phishing simulator and education solution.