Knowall Cloud

Phishing Emails

Protect Your Business

KNOWALL

PRIVATE CLOUD COMPUTING

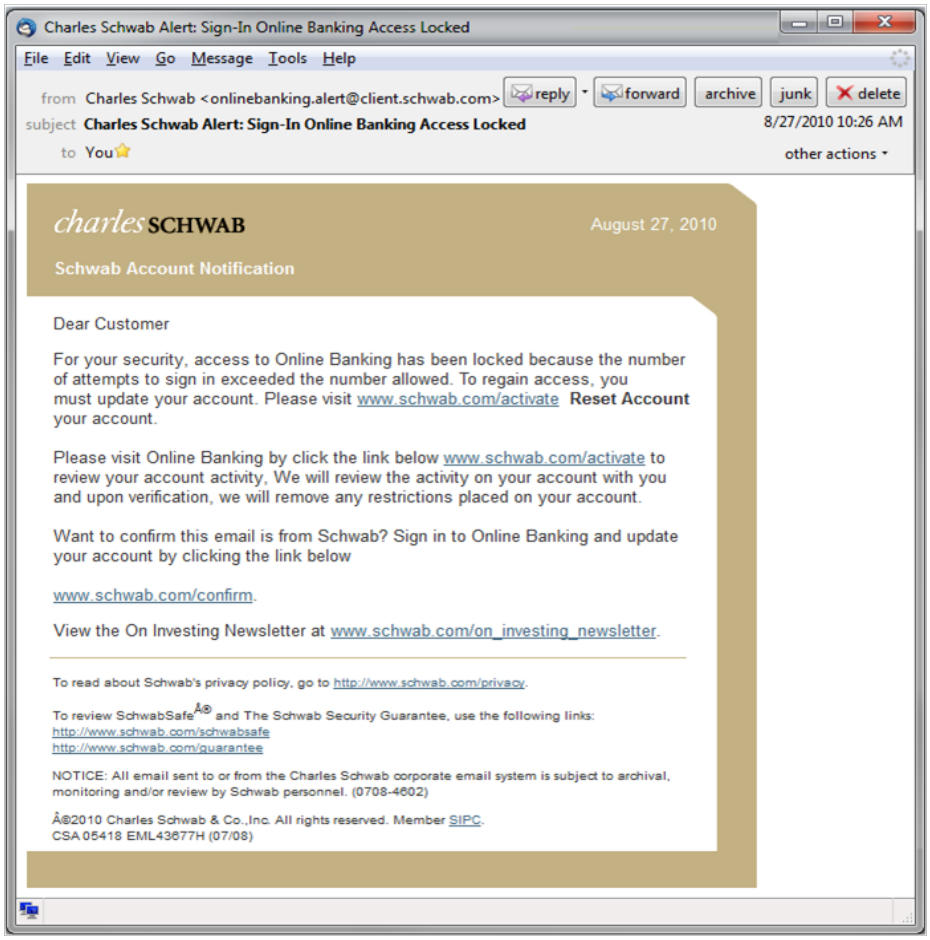
PHISHING EMAILS

Phishing is a type of online scam where criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information. This is usually done by including a link that will appear to take you to the company's website to fill in your information – but the website is a clever fake and the information you provide goes straight to the crooks behind the scam.

The term 'phishing' is a spin on the word fishing, because criminals are dangling a fake 'lure' (the email that looks legitimate, as well as the website that looks legitimate) hoping users will 'bite' by providing the information the criminals have requested – such as credit card numbers, account numbers, passwords, usernames, and more.

PHISHING EXAMPLE

See just how clever these phishing scams can be in the example below.



1. The email is not addressed to the recipient. If the recipient was truly being notified by that there was an issue with their account, they would know the recipient's name.

2. Again, they don't know the recipient's name;"Dear Customer" isn't an identifier.

3. The recipient hasn't attempted to sign into their account, so could not have exceeded the number of attempts allowed.

4. Grammatical errors: The words Online Banking are capitalized throughout the text. And, if you read carefully, the text says "Please visit www.schwab.com/activate Reset Account your account" which clearly doesn't make sense, but since most people scan emails quickly, grammatical errors that are this small usually don't get noticed.

5. They try to reassure recipients by encouraging them to confirm the email is from their account provider by using a link they provide.

Seeing any of the above flaws is enough to tell you the email is a phishing attempt – but what if these errors aren't present?

A smarter scammer could have corrected all these mistakes, including knowing the recipient's name and email address, and masking their URL in a much more convincing manner. If they had done a better job there would have been nothing in the message to trigger your alarm bells – even though the email would still be fake.

So how can you guarantee you protect yourself from phishing emails?

FORCEPOINT EMAIL SECURITY

Forcepoint Email Security is an on-premise, appliance-based system that prevents malicious email threats from entering an organisation's network, and protects sensitive data from unauthorised email transmission.

Forcepoint Email Security uses the Advanced Classification Engine (ACE) to identify threats ranging from annoying spam to advanced malware, phishing, and Business Email Compromise (BEC) attacks. Advanced capabilities detect data theft concealed in images or custom-encrypted files, even when gradually transmitted in small amounts to evade detection.

This application can also identify high-risk user behaviour. The rich data collection capability can quickly generate a report on Indicators of Compromise to identify infected systems and suspicious user behaviour.

ADVANTAGES

1. Real-time Threat Protection

Real-time threat protection uses a unique blend of detection technologies, including machine learning, sandboxing, and predictive analytics to effectively stop advanced threats such as ransomware.

2. Protection against highly evasive zero-day threats

Get advanced malware detection (sandboxing) with our full system emulation sandbox. Deep content inspection reveals highly evasive zero-day threat with no false positives.

3. Powerful encryption for additional protection

Encrypt sensitive email conversations and enhance mobile security by controlling sensitive attachments access by device.

4. Incident risk ranking to find the greatest risks

Incidents are correlated across multiple events to identify true cumulative risk trends and activity. A risk score is included to help security teams identify the greatest risks based on real-time activity.

5. Integrated data loss prevention

Integrated industry-leading data loss prevention stops data infiltration and exfiltration capabilities.

6. Unique phishing education feature

Use Forcepoint Email Security’s unique phishing education features to help users adopt best practices and identify those who need additional training to improve their security awareness.

7. Complete out-of-the-box solution

Forcepoint Email Security includes DLP, URL wrapping, and other capabilities that are considered premium "add-ons" or upgrades by many competitors, delivering the most comprehensive inbound and outbound defences out of the box.

8. Deployment flexibility

How you deploy our email security solution is up to you. Choose from a range of physical and virtual appliances to leverage existing hardware, cloud deployment, or hybrid environments.