GreatHorn

Get the facts on ...

Malicious URLs

Cybercriminals frequently deploy bad hyperlinks as part of phishing attacks. But few organizations realize just how insidious malicious URLs can be. Find out how weaponized links can threaten your business – and how to protect your enterprise from harm.

EBOOK

April 2021

What Are Malicious URLs?

URLs are ubiquitous and easy to share, which makes them effective weapons in the cybercriminal's arsenal. Just how many are out there? Every second of every day, 47 domain names are registered – nearly 1.5 billion per year, according to Verisign data.[1]

So it's no wonder cybercriminals deploy malicious URLs in their phishing attacks against your employees. Hyperlinks embedded in email content can lead users to malicious websites that automatically deliver malware, harvest user credentials or steal other sensitive information.

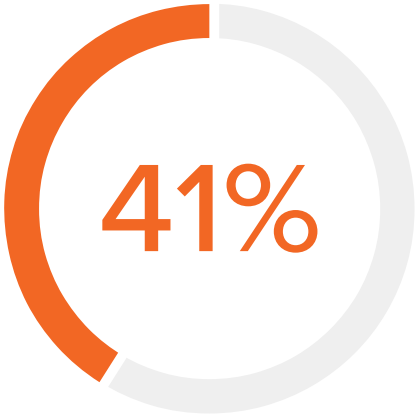
Malicious URLs are nefarious. Websites that appear to be safe when an email message is sent can later be weaponized with keystroke-logging malware or credential-harvesting forms. Such cyberattack vectors are a constant threat against your organization.

And, though "known bad" lists of URLs are available and used within many email security solutions, cybercriminals have found loopholes to land into user inboxes. One of these loopholes is to develop a non-malicious URL, which allows that hyperlink to process through the security solution and deliver it to the end user. Then, after the email is delivered, the cybercriminal weaponizes the URL with a malicious payload/credential harvesting/etc.

[1] *"The Domain Name Industry Brief, Q4 2020," Verisign, March 2021*

Data and Trends

Of organizations lack confidence users will avoid clicking on malicious links in their inbox.



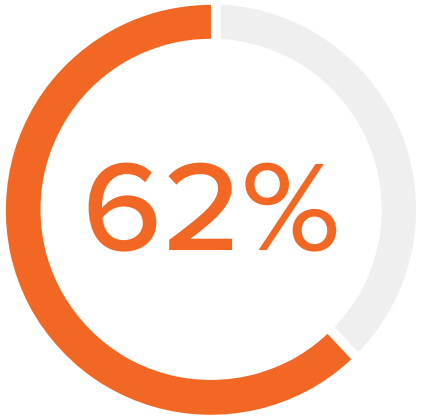
Say users click on malicious links on a daily basis.

3.7%

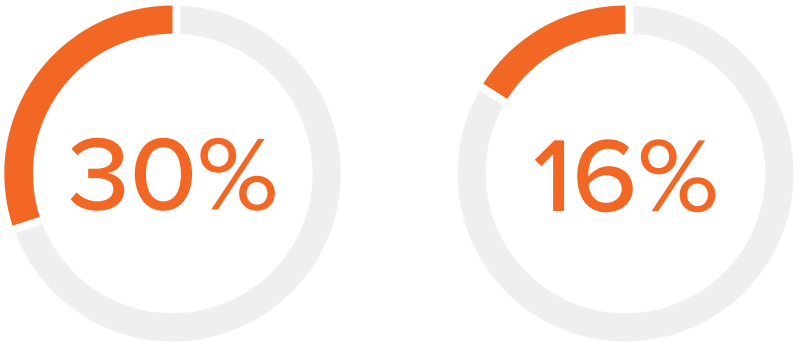
Of all emails contain a potentially malicious link that bypass native email security controls.

Source: GreatHorn Survey of 250 U.S. Cybersecurity Pros, March 2021

Data and Trends



Provide users with awareness training to discourage them from clicking on links.



Conduct awareness training at onboarding.

Conduct awareness training annually.

Source: GreatHorn Survey of 250 U.S. Cybersecurity Pros, March 2021

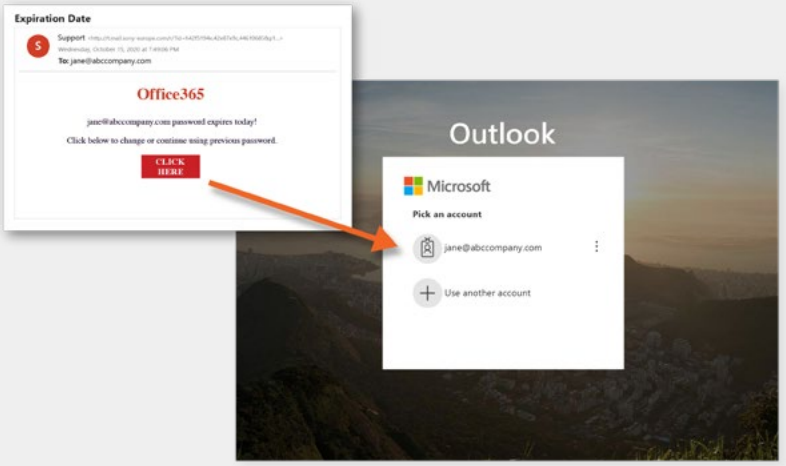
For more information about malicious payloads and ransomware attacks, read this eBook.

Example Attack

There are a multitude of different tactics and techniques cybercriminals leverage when incorporating hyperlinks into their phishing campaigns or BEC attacks. Here are a few examples that show the length cybercriminals go to bypass traditional email security solutions.

Redirector Attack Using URLs

A widespread cyberattack was identified that propagated through open redirector domains and subsidiary domains belonging to multiple global brands such as Sony, TripAdvisor and RAC. The attack involved multiple hosting services and webservers, which were used to host fraudulent Microsoft 365 login pages. Phishing emails containing malicious URLs bypassed email providers' native security controls and slipped past nearly every legacy email security platform. The attackers evaded detection by spoofing well-known applications such as Microsoft Office, Microsoft Teams, Zoom and others.



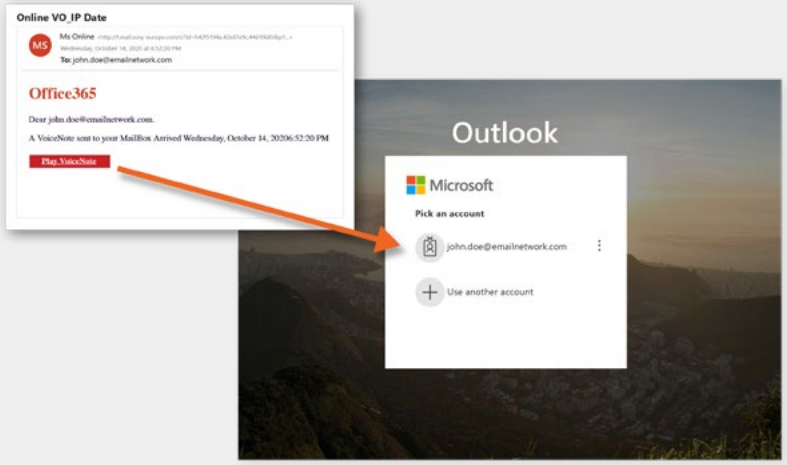
The malicious URLs were designed to steal corporate email credentials. They also deployed malware on the devices of users who visited the sites, even if the users didn't submit credentials.

For detailed information on this attack and to identify whether your organization was targeted, read this blog.

Malformed URL Prefixes

A new email attack trend using URLs that are malformed, i.e. not utilizing the normal URL protocols, such as http:// or https://. Instead, they use http:/\ in their URL prefix. Attackers identified that legacy email scanners do not do detect these malformed URL prefixes because the URLs don't fit the "known bad" profiles developed by simple email scanning programs. They may also slip past human eyes that aren't accustomed to looking in the prefix for signs of suspicious activity.

This specific phishing attempt impersonates a voicemail service, informing the recipient that they have a voice message. It emulates the appearance and behavior of many email platforms that use cloud-based voicemail services.



If the user then enters both their username and password, they'll be providing scammers with their login credentials. The attackers can then gain access to the recipient's email contact lists and other sensitive data, including cloud storage.

For detailed information on this attack and to identify whether your organization was targeted, read this blog.

Actions You Can Take Today

Cybercriminals typically carry out malicious-URL attacks through phishing – fraudulent email that purports to come from a reliable source. To protect your organization, you need an email security solution specifically designed to defend against these attacks.

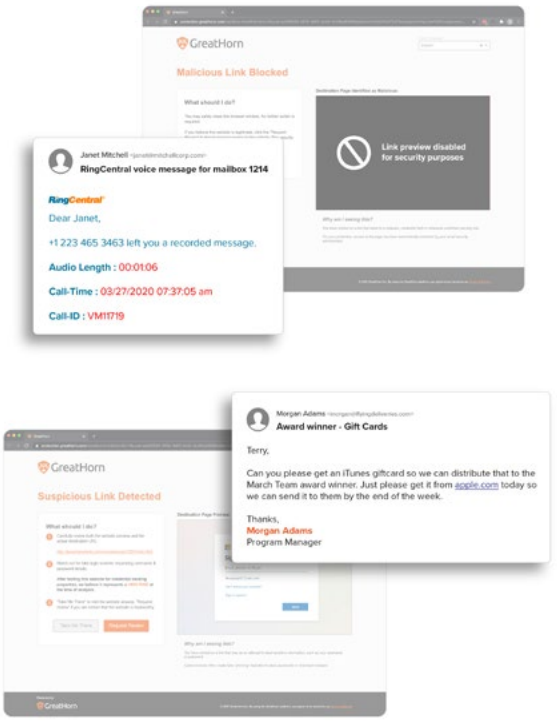
Your solution should combine threat intelligence, advanced spoof detection and a deep understanding of your organization's communication patterns. Automated controls should adapt to your unique risk requirements to take appropriate action – for example, quarantining emails, displaying user alerts or redirecting to a safe page at the moment the user clicks. Look for a solution that offers this crucial functionality:

- **Malicious URL Detection**
  Malicious URLs are a primary vector in phishing attacks, and it's easy for attackers to manipulate URLs so that no two appear the same. Your email security should inspect all URLs on delivery to identify links to malicious websites. It should also apply time-of-click analysis and computer vision to protect against links to websites that appear to be safe on delivery but are later weaponized with malware.

- **Suspicious URL Detection**
  Computer vision applies sophisticated technology to detect anomalous content, including potentially malicious content at URL destinations. If users click on a suspicious link, they can be redirected to a link-protection page that educates them with a preview of the destination page, the risk of credential harvesting and steps they should take to minimize their risk.

- **Behavioral Analytics**
  The solution should leverage sophisticated machine-learning (ML) algorithms to analyze all communication sequences between senders and recipients. Adaptive threat analytics can quickly and automatically learn user-specific interaction patterns and then instantly spot anomalous emails, hyperlinks and attachments that typify suspicious content.

- **User Education**
  Effective user education can provide your employees with the knowledge and context they need to avoid malicious URLs. Automated alerts and banners, mailbox intelligence and link-protection pages can help users understand threats, make informed decisions and take safe actions.



Ready to get control over malicious URLs? Contact GreatHorn now to simplify your response to phishing attacks.

About GreatHorn

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fast moving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.

v2021.04