

Human Hacking Through Phishing & Stolen Credentials

Prepared by Mark Viglione



Discussion Points

1. Hacking The Human

- What this means
- Why Threat Actors use this method

2. Phishing

- What it is and what to look out for in suspicious emails

3. Credentials

- What they are
- Why threat actors want them

4. Prevention & Remediation

- Recommendation for detect & prevent phishing & credential theft

HACKING THE HUMAN

People are the weakest security link in most business processes


You can secure your networks, computers and systems

- Making it more difficult for Malicious Actors to access

Employees opening and responding to emails that request action is a manual process

- Can't always control

Quicker (and easier) for cybercriminals to leverage people to gather intel and 'hack' their way into your network



How?



Phishing Scams

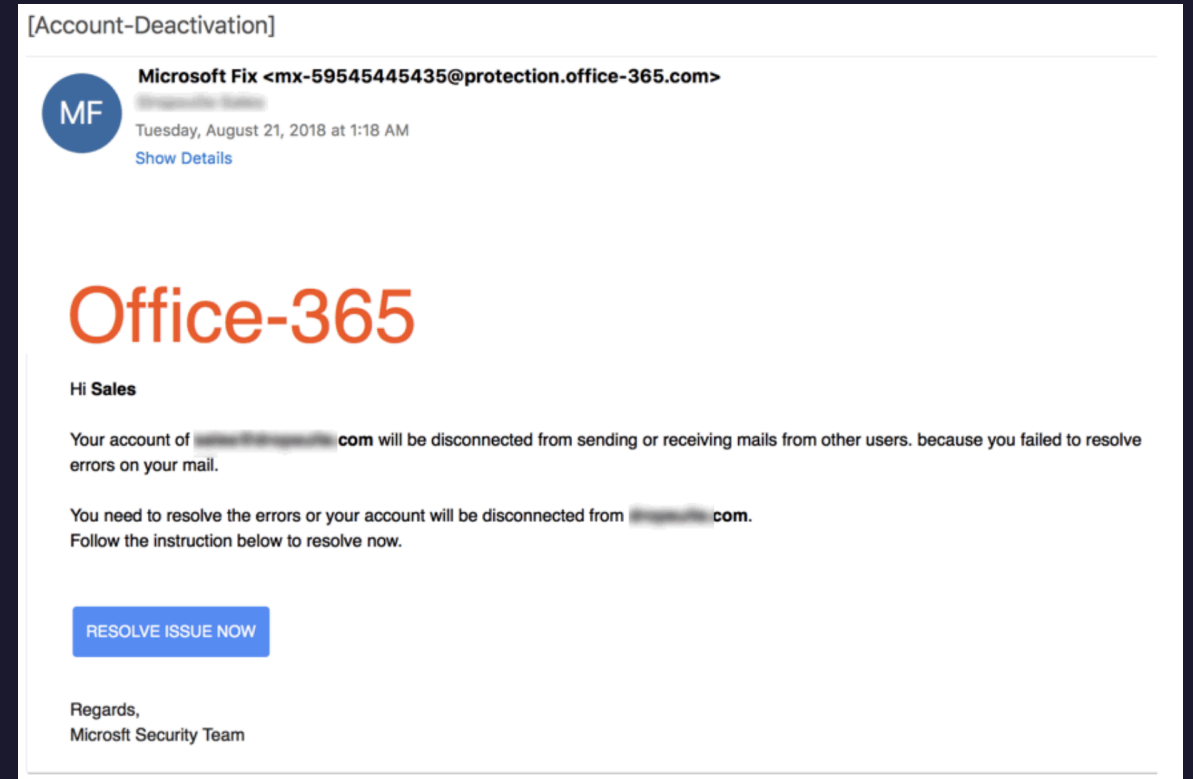


PHISHING

A cybercrime in which a target (or targets) are contacted by email, telephone or text message by someone posing as a legitimate institution

To lure individuals into providing malicious actors sensitive data such as personally identifiable information, banking and credit card details, and passwords

The information is then used to access important accounts and can result in identity theft and financial loss



“Phishing is more than 20 years old, but still represents more than 90% of targeted attacks. The reason is simple: it works” - Proofpoint

Common Features of Phishing Emails

1. Sense of urgency

- Want you to act quickly so you make less informed decisions

2. Unusual sender

- Spoofed domain names, fake company addresses, etc.

3. Too good to be true

- Lucrative offers and eye-catching statements (e.g. free iPhone) – If it seems too good to be true, it probably is...

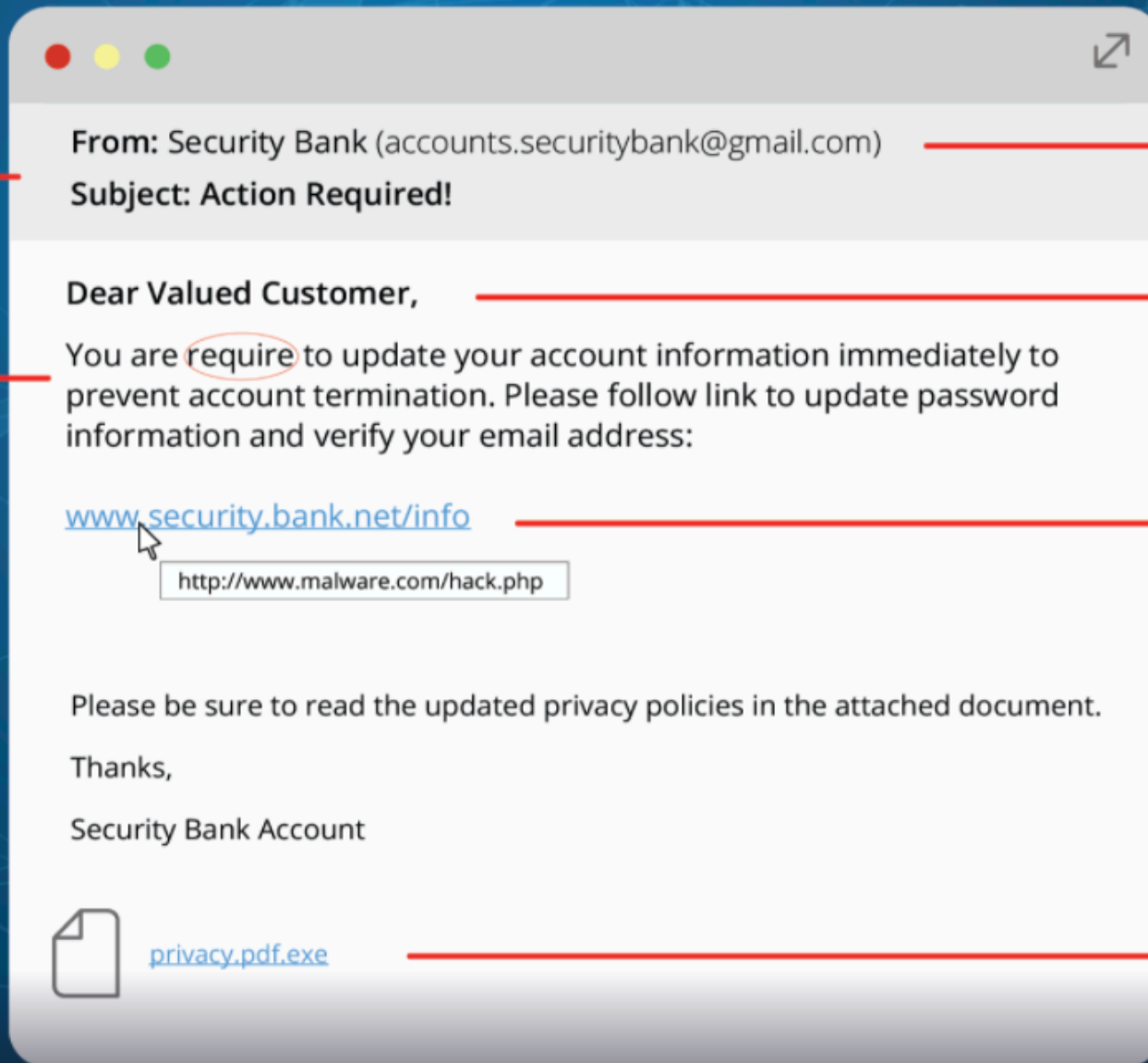
4. Suspicious attachments and hyperlinks

- Attachments can contain malicious payloads (ransomware, macros, etc.), links can lead to malicious web pages

WATCH OUT FOR...

a sense of urgency

spelling & grammar mistakes



an illegitimate or unfamiliar address

a generic greeting or salutation

suspicious links or links that don't match the destination

unexpected attachments (especially files ending in .exe)

Result of a Successful Phish



CREDENTIALS

What are they?

- Any specific data or authentication tool required to verify the identity of a user, authenticate them and grant access to a system or network

What do cybercriminals do after they harvest them?

- To achieve their final goal (some form profit) – cybercriminals usually have one of the following objectives:
 1. Fraud: account takeovers, money transfers and purchases, money laundering
 2. Blackmail: sensitive information is not sold, but rather ransomed back to the original owners
 3. Reputation damage: harm to the image of your company
 4. Sell: on the dark web
 5. Lateral movement: use the stolen creds to access various resources and data within your internal network

PREVENTION & REMEDIATION

Many tools & services on the market

Find the right tools that can augment your existing business processes to enable stronger security controls

No silver bullet

The right tools combined with strong security policies can reduce your vulnerabilities and mitigate threats

Confused by Cybersecurity?



Combating Phishing Attacks

1. Reduce your attack surface

- Deploy tools that monitor and analyze email messages, URLs, attachments
- Provide user click statistics (so you can see what types of emails your employee are opening/clicking on)

2. Provide quarterly end-user phishing training

- Perform a phishing simulation and use tools to track users who clicked
- Understand what they opened/clicked and why they did

3. Obtain better visibility into your IT environment

- Having a simple dashboard that shows what normal activity looks like will help identify anomalous activity

Preventing Credential Theft

1. Ensure employees are leveraging multifactor authentication (MFA)
 - If an employee enters their business creds into a malicious web page, the attacker still needs MFA code
2. Understand who has privileged accounts and administrative access to sensitive systems
3. Deploy monitoring tools to detect suspicious account activity
 - Abnormal login requests, high failed logins – can all be signs of brute force and unauthorized access attempts
4. If a user/system is compromised
 - Isolate the device from the network, reset the user's credentials immediately

Thank You!



Simplifying Cybersecurity for Small to Midsized Businesses

Mark Viglione, Founder

Phone: 610-805-4354

Email: mark@enigmanetworkz.com

Website: <https://enigmanetworkz.com>