Why Phishing Works

A successful phishing attack accomplishes two basic goals: *it gains the trust of victims and exploits their emotions.*

Imagine a friend of yours is looking for a job. She posts her resume on various sites and sends out applications. Then, she finally receives an email, that appears to come from Linkedin, with a great job offer. *All your friend has to do is click the link and upload her personal details. But is it a scam?* More importantly, would your friend, who has been on the job hunt for several months, even question its authenticity?

Now let's flip roles. Let's say you handle the hiring of new employees and you get lots of emails from applicants with attachments. *How difficult would it be for a social engineer to push a malicious attachment, disguised as a resume, to your inbox?*

What about emails that appear to come from someone you know?

Trust, desperation, and fear are the most effective weapons of scammers.

As always:

- If you do not recognize the sender or are not expecting an email, *delete it.*
- It is important to verify the details in the message before responding.
- Always *hover over the web link before clicking* to see if the link takes you to the correct site.
- On mobile devices, tap and hold on the link to preview the web address
- If you are unsure, follow the County's policies and report it by clicking on the Report Phishing CRISI button in the Outlook Home tab.

Phishing Identification Checklist

- ☐ Does the email contain poor spelling and/or bad grammar?
- ☐ Is the email awkwardly worded ?
- ☐ Is the "from" address unrecognizable or just plain weird?
- ☐ Does the email promise large sums of money or other unbelievable offers?
- ☐ Does the email use threatening language?
- ☐ Does the email contain a sense of urgency?
- ☐ Does the email have a call-to-action such as clicking a link?
- ☐ Does the email contain an unexpected attachment or request for money?

If you had to check any of these boxes, beware! It could be a phishing email.

Protect the County and yourself
Do not click on links or open attahments from emails you are not expecting, or from companies you do not do business with.

DID YOU KNOW...

Email addresses can be spoofed, or forged, to make messages appear to come from legitimate sources. Victims are much more likely to cooperate when they believe they are communicating with someone they know, which is even more reason to fully scrutinize all requests for sensitive info or money!